TUPELSYSTEME - EINE GEMEINSAME THEORIE FÜR BLOCKPLÄNE UND ORTHOGONALE ARRAYS

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

des

Fachbereich 19/Mathematik

der Freien Universität Berlin

1977

vorgelegt

im Jahre 1976

von

Arnold Neumaier

aus

Dettenhausen

UNIV.
LEIDEN
BIBL.

1.Referent: Prof.Dr. M.Aigner

2.Referent: Prof.Dr. H.Lenz

Tag der Promotion: 12.1.77

Reprinted from JOURNAL OF COMBINATORICS, INFORMATION & SYSTEM SCIENCES

Vol. 2, No. 2/3, 41–96 (1977)
Printed in India

Tupelsysteme—Eine gemeinsame Theorie für Blockpläne und Orthogonale Arrays

ARNOLD NEUMAIER

2. Math. Institut der Freien Universität Berlin,
Königin-Luise-Str. 24–26, D-1000 Berlin 33, West-Germany

The paper tries to develop a uniform theory of balanced incomplete block designs, orthogonal arrays, and some other combinatorial configurations by introducing the new notion of a tuple system. The theory concentrates on two strongly related types of tuple systems, namely strong balanced tuple systems (SBTS), and homogeneous tuple systems (HTS).

If $M=(\mu_{ij})$ is a $k\times k$-matrix with positive entries, and if G is a faithful permutation group of degree k, then a $(v, k, \mu, M; G)$-SBTS is a multiset Q of k-tuples with distinct entries out of a v-set P such that (1) The number of tuples $x \in Q$ with $x_i = a$ is constantly $\mu(v-1)$, (2) The number of tuples $x \in Q$ with $x_i = a$, $x_j = b$ $(i \neq j)$ is either 0 or μ_{ij}, (3) For every $\alpha \in G$ the tuple αx (obtained from x by reordering the entries according to α) appears in Q with the same multiplicity as x.

Similarly, a $(v, k, \mu; G)$-HTS is a multiset Q of k-tuples with (not necessarily distinct) entries out of a v-set P such that (2a) the number of tuples $x \in Q$ with $x_i = a$, $x_j = b$ is constantly μ, (3) as above.

If every tuple $(a, \ldots, a)$ is added μ times to a $(v, k, \mu; G)$-SBTS (i.e. a SBTS with $\mu_{ij} = \mu$ everywhere) then a $(v, k, \mu; G)$-HTS is obtained.

Several equivalence theorems relating HTS or SBTS to classical combinatorial concepts are given. The paper provides constructions for HTS and SBTS by algebraic means, by the method of differences, and by recursive methods. Moreover, some theorems are proved concerning the existence of SBTS for large v, and a survey of SBTS with $k = 3, 4$ concludes the paper.

There remain a lot of interesting problems with regard to the existence and construction of HTS and SBTS.

1. EINFÜHRUNG

Diese Arbeit stellt den Versuch dar, verschiedene kombinatorische Strukturen von einem einheitlichen Gesichtspunkt aus zu betrachten. Seit etwa 1960 sind für verschiedene Strukturen gleichartige Arbeitsmethoden, Konstruktionsverfahren und Existenzbeweise entwickelt worden (z.B. die PBD-Konstruktion, die Moore-Konstruktion, Differenzenverfahren, das singular direct product und jeweils damit zusammemhängende Existenzsätze). Wir

© Forum for Interdisciplinary Mathematics.
No part of this publication may be reproduced in any form without written permission of the Chief Editor.

1977

arbeiten diese gemeinsame Grundstruktur im folgenden heraus durch die Einführung eines neuen Begriffs: des Tupelsystems.

Im Prinzip ist ein Tupelsystem nichts anderes als eine (Multi-)Menge Q von k-Tuplen über einer Punktmenge P. Der Begriff des Tupelsystems ist ein sehr allgemeiner Rahmen für kombinatorische Designs, ähnlich umfassend wie der der Inzidenzstruktur. Durch zusätzliche Axiome werden die interessanten Tupelsysteme definiert. Die Richtung der Interpretation wird festgelegt, indem wir uns besonders auf Forderungen an die sog. Situationszahlen ($\rho_i(a)$ = Anzahl der Tupel $x \in Q$ mit $x_i = a$, $\mu_{ij}(a, b)$ = Anzahl der $x \in Q$ mit $x_i = a$, $x_l = b$ $(i \neq j)$) konzentrieren. Daß wir hier höchstens zwei Stellen (i und j) in Betracht ziehen, ist an sich keine notwendige Einschränkung, jedoch hat bisher nur dieser Fall zu einer einigermaßen geschlossenen Theorie geführt. Die Forderung, daß $\mu_{ij}(a, b)$ konstant ist, führt zu homogenen Tupelsystemen (HTS), und die Forderung, daß $\mu_{ij}(a, b)$ für $a \neq b$ konstant und für $a = b$ Null ist, definiert streng balancierte Tupelsysteme (SBTS).

Eine Reihe von Äquivalenzsätzen charakterisiert nun bekannte kombinatorische Strukturen innerhalb dieses Begriffs-systems. Die folgenden Strukturen lassen sich als spezielle Tupelsysteme darstellen:

1. Blockpläne (Abschnitt 3.4)
2. Orthogonale Arrays (Abschnitt 3.3)
3. Orthogonale Lateinische Quadrate und Quasigruppen (3.3)

3a. Selbstorthogonale Lateinische Quadrate (3.3)

4. Transversalpläne (3.1)
5. Netze (3.2)
6. auflösbare und affine Blockpläne (3.2)
7. Hadamardmatrizen (s. Anhang)
8. Roomsche Quadrate (3.5)
9. (semireguläre) group divisible designs (s. Anhang)
10. Equidistante Blockcodes mit Hammingdistanz $d = k - 1$ (s. Anhang)

Diese Aufzählung gibt einen guten Begriff von der Reichweite der neuen Definition.

Nach den Äquivalenzbeweisen wenden wir uns der Konstruktion von homogenen und streng balancierten Tupelsystemen zu. Die verwendeten Methoden sind algebraische (direkte Konstruktionen aus Körpern), zahlentheoretische (Starterkonstruktion, method of differences) und kombinatorische (rekursive Konstruktionen). Während die algebraischen Methoden nur spezielle Tupelsysteme liefern, bilden die Starter-und rekursiven Konstruktionen einen allgemeinen Rahmen. Die rekursiven Methoden lassen sich systematisieren; wir können jedoch in dieser Arbeit nicht darauf eingehen.

Schließlich verallgemeinern wir Existenzsätze, die in den Randfällen der orthogonalen lateinischen Quadrate von Bose, Shrikhande und Parker [2], und für Blockpläne von Wilson [28–30] stammen. Die dort erzielten Ergebnisse gehen auch stark in unsere Beweisführung ein. Allerdings gelingt es uns nicht in allen Fällen, notwendige und hinreichende Existenzbedingungen (für große v) zu beweisen. Zum Schluß geben wir einen Überblick über die Existenzfrage für $k = 3$ und $k = 4$; es zeigt sich, daß die nichtklassischen Fälle noch zahlreiche reizvolle Konstruktionsprobleme bieten.

Um dem Leser einen Begriff vom Wesen der Tupelsysteme und ihrer Beziehung zu klassischen kombinatorischen Strukturen zu geben, vergleichen wir die Eigenschaften von Blockplänen und Orthogonalen Arrays.

Ein Blockplan ist eine (Multi-)Menge von Teilmengen ("Blöcken") einer endlichen Menge (von "Punkten") mit den Eigenschaften (B1) Jeder Block enthält genau k Punkte, und (B2) Jedes paar verschiedener Punkte liegt in genau λ Blöcken.

Eine orthogonale Array (der Stufe 2) ist eine $\mu v^2 \times k$-Matrix M mit Elementen aus einer endlichen Menge P (von "Punkten") mit den Eigenschaften (O1) Jede Zeile enthält genau k Punkte, und (O2) Jedes Paar von (nicht notwendig verschiedenen) Punkten liegt auf vorgegebenen Spalten in genau μ Zeilen der Matrix (für jede Auswahl der Spalten). (O1) ist natürlich eine triviale Bedingung, die nur die Ähnlichkeit der Definition mit der für die Blockpläne hervorheben soll.

Man sieht sofort, daß die Reihenfolge der Zeilen der Matrix unerheblich ist. Deshalb lassen wir die Anordnung der Zeilen in der Matrix fallen und betrachten anstelle von M die (Multi-)Menge Q_{OA} der Zeilen. Jede einzelne Zeile ist jetzt ein k-Tupel von Punkten, Q_{OA} also ein Tupelsystem. $Q = Q_{OA}$ erfüllt die Bedingung (H2) Die Zahl der Tupel $x \in Q$, deren i-te Stelle mit a, und deren j-te Stelle mit b besetzt ist, ist μ, unabhängig von der Wahl der Punkte a, b und der Stellen i, j $(i \neq j)$.

Das neue Tupelsystem ist einem Blockplan schon ähnlicher. Jetzt versuchen wir, auch noch die unterscheidung von k-Tupeln und k-Blöcken aufzuheben: Wir ordnen die Punkte jedes Blocks aus dem Blockplan in irgendeiner Weise an. Um uns von der Willkür, die darin liegt, zu befreien, nehmen wir zu diesen Tupeln jetzt noch alle Permutationen dieses Tupels hinzu. Auf diese Weise erhalten wir eine eineindeutige Zuordnung zwischen Blöcken und bestimmten Mengen von k-Tupeln.

Wir fassen nun alle diese Tupel zu einem Tupelsystem Q^o zusammen. Dann erfüllt Q^o die Bedingung (H2) mit $\mu = \lambda(k-2)!$ für alle $a \neq b$. Wenn wir zu Q^o noch μ-mal jedes Tupel $(a, \ldots, a)$ hinzufügen, entfällt auch diese Einschränkung. Das entstandene Tupelsystem soll Q_{BIBD} sein.

Jetzt sind beide Begriffe, der Blockplan und die Orthogonale Array, auf dasselbe kombinatorische Konzept zurückgeführt. Enthält P genau v

Punkte, so nennen wir eine (Multi-)Menge Q von k-Tupeln, die (H2) erfüllt, ein (v, k, μ)-HTS (homogenes Tupelsystem).

Wo liegen die Unterschiede zwischen Q_{OA} und Q_{BIBD}? $Q = Q_{BIBD}$ hat zwei zusätzliche Eigenschaften. Erstens enthält Q jedes Tupel $(a, \ldots, a)$ genau μ-fach. Ein solches HTS nennen wir idempotent. Zweitens hat jede Permutation α der k Stellen die Eigenschaft (A) Das Tupel αx (das aus x durch die α entsprechende Umordnung der Einträge entsteht) tritt in Q mit derselben Häufigkeit auf wie das Tupel x selbst. Eine Permutation der Stellen, die (A) erfüllt, nennen wir einen freien Automorphismus von Q. Die zweite Eigenschaft ist also, daß Q_{BIBD} die symmetrische Gruppe S_k als freie Automorphismengruppe hat.

So erscheinen also die beiden Begriffe als die Extremfälle eines total unsymmetrischen HTS (triviale freie Automorphismengruppe $\triangleq$ orthogonale Array) und eines totalsymmetrischen idempotenten HTS (symmetrische Gruppe als freie Automorphismengruppe $\triangleq$ Blockplan). Dazwischen erstreckt sich der Bereich der Homogenen Tupelsysteme mit irgendeiner vorgegebenen freien Automorphismengruppe, deren Untersuchung eine der Aufgaben der vorliegenden Arbeit ist.

Als historische Bemerkung sei zum Schluß erwähnt, daß in einer 1896 (!) erschienenen Arbeit [16] E. H. Moore—im Zusammenhang mit Whist-Turnieren—schon Beispiele für $(v, 4, 1; V_4)$-HTS und $(v, 4, 2; D_4)$-HTS (mit der Kleinschen Veirergruppe V_4 bzw. der Diedergruppe D_4 vom Grad 4 als freier Automorphismengruppe) angegeben hat.

2. DEFINITIONEN

Wir führen in Abschnitt 2.1. den Begriff des Tupelsystems ein, Unter den Tupelsystemen definieren wir zwei Äquivalenzrelationen, Isotopie und Isomorphie. Autotopismen und Automorphismen werden eingeführt, insbesondere die im folgenden wichtigen freien Automorphismen. Ein Beispiel verdeutlicht die neuen Begriffe.

Abschnitt 2.2. enthält die Definitionen und einfache Sätze über grundlegenden Strukturen dieser Arbeit: Stark balancierte Tupelsysteme (SBTS) und Homogene Tupelsysteme (HTS). Es werden notwendige Bedingungen für die Existenz von SBTS abgeleitet, und der Zusammenhang zwischen den beiden Begriffen erörtert. Außerdem wird eine Ungleichung für die Parameter eines HTS bewiesen.

Abschnitt 2.3. ist ein kurzer Abriß der Theorie der PBD (pairwise balanced designs) und der Blockpläne. Hier werden die Definitionen und Sätze zusammengestellt, die später benötigt werden.

2.1. TUPELSYSTEME

2.1.1. *Definition* (*Tupelsystem*). Ein Tupelsystem ist ein Quadrupel (P, I, Q, ϵ), bestehend aus einer Menge P von "Punkten", einer Menge I von

"Stellen" und einer Abbildung $\epsilon : Q \times I \to P$ (Belegung, occupation map). Anstelle von $\epsilon(x, i)$ schreiben wir i.A. einfach x_i.

Die Vereinigung zweier Tupelsysteme (P, I, Q, ϵ) und (P, I, Q', ϵ') mit $Q \cap Q' = \emptyset$ ist das Tupelsystem $(P, I, Q \cup Q', \epsilon^*)$, wo $\epsilon^*(x) = \epsilon(x)$ wenn $x \in Q$, und $= \epsilon'(x)$ wenn $x \in Q'$ ist.

Wir betrachten nur endliche Tupelsysteme, in denen also P, I und Q endlich sind. Ist $|P| = v$, $|I| = k$, so heißt das endliche Tupelsystem (P, I, Q, ϵ) ein (v, k)-Tupelsystem. In diesem Fall identifizieren wir x mit dem k-Tupel $(x_i : i \in I)$. Q wird damit zu einer Multimenge von k-Tupeln über P, und wird auch ein (v, k)-Tupelsystem über P (oder kurz ein (P, k)-Tupelsystem) genannt.[1] Entsprechend dieser Übereinkunft werden oft nur Q, stellvertretend für (P, I, Q, ϵ) schreiben.

Wir begnügen uns mit dem intuitiven Begriff der Multimenge als einer Menge, in der jedes Element mit einer bestimmten Vielfachheit auftreten kann, und bemerken nur, daß wir die Vereinigung $M \cup N$ zweier Multimenger bilden, indem wir die entsprechenden Vielfachheiten addieren.

Bemerkung. Obwohl die Definition des Tupelystems zunächst symmetrisch in Q und I ist, wird durch die gegebene Interpretation eine wesentliche Asymmetrie geschaffen.

2.1.2. *Definition* (*Isotopie, usw.*). (P, I, Q, ϵ) und (P', I', Q', ϵ') seien (v, k)-Tupelsysteme. Ein Paar (α, π), bestehend aus einer Bijektion $\alpha : I \to I'$ und einem k-Tupel $\Pi = (\pi_i : i \in I)$ von Bijektionen $\pi_i : P \to P'$ heißt ein Isotopismus von Q auf Q', wenn eine Bijektion $\phi : Q \to Q'$ existiert mit der Eigenschaft

$$\epsilon(x, i) = a \Leftrightarrow \epsilon' (\phi x, \alpha i) = \pi_i a \text{ für alle } x \in Q, i \in I, a \in P.$$

Wir nennen den Isotopismus (α, π) rein, wenn $\alpha = 1$.

Ein Isomorphismus von Q auf Q' ist ein Isotopismus (α, Π) mit $\Pi = (\pi : i \in I)$. Ein solcher heißt rein, wenn $\alpha = 1$, und frei, wenn $\pi = 1$ ist.

Q und Q' heißen isotop (isomorph), wenn ein Isotopismus (Isomorphismus) von Q auf Q' existiert.

Ein Autotopismus (Automorphismus) von Q ist ein Isotopismus (Isomorphismus) von Q auf sich selbst.

Bemerkung. In der Multimengenschreibweise ist (α, π) genau dann ein Isotopismus von Q auf Q', wenn das Tupel

$$(\alpha, \Pi)x = (\pi_{\alpha^{-1}i} x_{\alpha^{-1}i} : i \in I)$$

in Q' mit derselben Vielfachheit auftritt wie x in Q. Die entsprechende

1. Wie hier ersetzen wir auch im Folgenden mehrfach einen Zahlenparameter durch die entsprechende Menge.

Zuordnung ϕ der Tupel ist genau dann eindeutig bestimmt, wenn Q als Multimenge sogar Menge ist. In diesem Fall schreiben wir für ϕ ebenfalls (α, Π). Im Allgemeinfall rechtfertigt die Mehrdeutigkeit von ϕ, daß wir ϕ nicht in die Beschreibung des Isotopismus mit aufgenommen haben.

Wir schreiben für einen reinen Isotopismus $(1, \pi)$ nur π, für einen Isomorphismus (α, Π) mit $\Pi = (\pi : i \in I)$ einfach (α, π), und für einen reinen (freien) Isomorphismus $(1, \pi)$ bzw. $(\alpha, 1)$ einfach π bzw. α.

Die freien Automorphismen eines Tupelsystems spielen in der Theorie eine wichtige Rolle. Das liegt daran, daß in vielen Konstruktionen eine Gruppe freier Automorphismen vorgegeben werden kann, und daß mehrere rekursive Konstruktionen die Gruppe der freien Automorphismen erhalten.

2.1.3. (a) Isotopie und Isomorphie sind Aquivalenzrelationen.

(b) Die Autotopismen eines Tupelsystems Q bilden eine Gruppe $\mathrm{Aut}_o(Q)$ bezüglich der Operation $(\alpha, \pi)\cdot(\alpha', \pi') = (\alpha\alpha', \pi^*)$ mit $\pi^* = (\pi_{\alpha' i}\, \pi_i' : i \in I)$. Die reinen Autotophismen bilden einen Normalteiler $\mathrm{Aut}_{or}(Q)$ von $\mathrm{Aut}_o(Q)$.

(c) Die Automorphismen von Q bilden eine Untergruppe $\mathrm{Aut}(Q)$ von $\mathrm{Aut}_o(Q)$; die reinen (freien) Automorphismen von Q bilden elementweise vertauschbare Normalteiler $\mathrm{Aut}_r(Q)$ bzw. $\mathrm{Aut}_f(Q)$.

Der Beweis wird dem Leser überlassen.

2.1.4. *Definition* (*Situationszahlen*). Ist (P, I, Q, ϵ) ein endliches Tupelsystem, so nennen wir die Zahlen $(a, c \in P; i, j \in I, i \neq j)$

$$
\begin{aligned}
b &= \text{Anzahl der Tupel } x \in Q,\\
\rho_i(a) &= \text{Anzahl der Tupel } x \in Q \text{ mit } x_i = a,\\
\mu_{ij}(a, c) &= \text{Anzahl der Tupel } x \in Q \text{ mit } x_i = a,\ x_j = c
\end{aligned}
$$

die Situationszahlen des Tupelsystems. (Falls nötig schreiben wir für die Situationszahlen auch b^Q, $\rho_i^Q(a)$, $\mu_{ij}{}^Q(a, c)$.)

2.1.5. *Beispiel.* K sei additiv geschriebene abelsche Gruppe der Ordnung v. Das Tupelsystem $Q = \{(a, b, c) \,|\, a, b, c \in K, a + b + c = 0\}$ hat die Situationszahlen $b = v^2$, $\rho_i(a) = v$, $\mu_{ij}(a, b) = 1$ (für alle $a, b \in K$; $i, j \in \{1, 2, 3\}$, $i \neq j$). Es ist $\mathrm{Aut}_o(Q) = S_3 \otimes \mathrm{Aut}_{or}(Q)$, $\mathrm{Aut}(Q) = S_3 \otimes \mathrm{Aut}_r(Q)$, $\mathrm{Aut}_f(Q) = S_3$. $\mathrm{Aut}_{or}(Q)$ besteht gerade aus den Tripeln (π_1, π_2, π_3) mit

$$\pi_i a = \sigma a + t_i (i = 1, 2, 3;\ a \in K), \text{ wo } \sigma \in \mathrm{Aut}\, K,\ t_1 + t_2 + t_3 = 0. \qquad (1)$$

Die Automorphismen von K sind reine Automorphismen von Q, und falls $3 \nmid v$ ist sogar $\mathrm{Aut}_r(Q) = \mathrm{Aut}\, K$.

Die Situationszahlen ergeben sich hier unmittelbar aus der Anzahl der freien Variablen; z.B. ist $\rho_1(a)$ die Zahl der $(a, b, -a - b)$ mit festem a, also $\rho_1(a) = v$.

Da die Definition von Q in a, b, c symmetrisch ist, ist jede Permutation

der Stellen ein freier Automorphismus, und daher $\mathrm{Aut}_f(Q) = S_3$, $\mathrm{Aut}_o(Q) = S_3 \otimes \mathrm{Aut}_{or}(Q)$, $\mathrm{Aut}(Q) = S_3 \otimes \mathrm{Aut}_r(Q)$. Es genügt nun zu zeigen, daß jeder reine Autotopismus (π_1, π_2, π_3) die Form (1) hat, da der Rest dann unmittelbar folgt.

Es gibt Elemente $t_i \in K$ und Permutationen σ_i von K mit $\sigma_i 0 = 0$, $\pi_i a = \sigma_i a + t_i$ $(i = 1, 2, 3)$. Wegen $(0, 0, 0) \in Q$ ist $\pi(0, 0, 0) = (t_1, t_2, t_3) \in Q$, also $t_1 + t_2 + t_3 = 0$. Analog folgt jetzt aus $(a, b, -a-b) \in Q$ die Bedingung $\sigma_1 a + \sigma_2 b + \sigma_3(-a-b) = 0$. Setzen wir nun $a = 0$ bzw. $b = 0$, so ergibt sich $\sigma_1 a = -\sigma_3(-a) = \sigma_2 a$, und wir erhalten mit $\sigma = \sigma_1$ die Beziehung $\sigma a + \sigma b = \sigma(a + b)$. Daher ist $\sigma \in \mathrm{Aut}\, K$. Aus $\sigma_3 a = -\sigma_1(-a) = -\sigma(-a) = \sigma a$ ergibt sich schließlich $\sigma_1 = \sigma_2 = \sigma_3 = \sigma$, also (1).

Achtung. Im Allgemeinen gilt nur $\mathrm{Aut}_o(Q) \supseteq \mathrm{Aut}_f(Q) \otimes \mathrm{Aut}_{or}(Q)$ und $\mathrm{Aut}(Q) \supseteq \mathrm{Aut}_f(Q) \otimes \mathrm{Aut}_r(Q)$!

2.2. Homogene und Stark Balancierte Tupelsysteme

$M = (\mu_{ij} : i, j \in I)$ sei eine symmetrische $k \times k$-Matrix, deren Diagonal-elemente 0 und deren übrigen Elemente natürliche Zahlen sind. G sei eine auf I treue Permutationsgruppe.

2.2.1. *Definition* (*Stark balanciertes Tupelsystem, SBTS*). Ein $(v, k, \mu, M; G)$-SBTS ist ein (v, k)-Tupelsystem (P, I, Q, ϵ) mit den Eigenschaften

(SBTS1) G ist Gruppe freier Automorphismen von (P, I, Q, ϵ)

(SBTS2) $\mu_{ij}(a, a) = 0$ für alle $a \in P$, $i, j \in I$, $i \neq j$,

(SBTS3) $\rho_i(a) = \mu(v-1)$, $\mu_{ij}(a, c) \in \{0, \mu_{ij}\}$ für alle $a, c \in P$, $i, j \in I$, $i \neq j$.

Ein $(v, k, \mu; G)$-SBTS ist ein (v, k)-Tupelsystem (P, I, Q, ϵ) mit den Eigenschaften (SBTS1), (SBTS2) und

(SBTS3a) $\mu_{ij}(a, c) = \mu$ für alle $a, c \in P$, $a \neq c$, $i, j \in I$, $i \neq j$.

Ist G trivial, so lassen wir G aus der Parameterliste aus.

Bemerkung. Aus (SBTS3) ergibt sich die Zahl der Tupel in Q zu $b = \sum_{a \in P} \rho_i(a) = |P| \mu(v-1) = \mu v(v-1)$.

Der Begriff des SBTS ist invariant gegenüber Isomorphismen (α, π). Dabei verändert sich M zu $M' = (\mu_{\alpha^{-1}i, \alpha^{-1}j} : i, j \in I)$, und G geht in die isomorphe Gruppe $\alpha G \alpha^{-1}$ über. Dagegen ist der Begiff des SBTS nicht invarient gegenüber Isotopismen, da (SBTS2) nicht erhalten bleiben muß!

Ein triviales, aber wichtiges Beispiel für SBTS ist das leere Tupelsystem $Q = \emptyset$ über einer einelementigen Menge P. Das ist ein $(1, k, \mu, M; G)$-SBTS für alle Parameter $k, \mu, M; G$. (Das sind zugleich alle SBTS mit

$v = 1$.). Für $v > 1$ müssen die Parameter jedoch bestimmten Einschränkungen genügen:

2.2.2. *Proposition.* Es sei $v \geqslant 2$, $k \geqslant 2$, $\mu \geqslant 1$. Ist dann $(P, I, Q, \in)$ ein $(v, k, \mu, M; G)$-SBTS, so gilt für alle $i, j \in I$, $i \neq j$:

$$\mu_{\alpha i, \alpha j} = \mu_{ij} = \mu_{ji} (\alpha \in G), \tag{1}$$

$$\mu \leqslant \mu_{ij} \mid \mu(v-1), \tag{2}$$

$$|G_{ij}| \mid \mu_{ij}, \quad |G_j| \mid \mu(v-1), \quad |G| \mid \mu v(v-1). \tag{3}$$

In (2) gilt die Gleichheit $\mu = \mu_{ij}$ genau dann für alle $i \neq j$, wenn Q ein $(v, k, \mu; G)$-SBTS ist.

Beweis. (a) (1) ergibt sich sofort aus $\mu_{\alpha i, \alpha j}(a, c) = \mu_{ij}(a, c) = \mu_{ji}(c, a)$ für alle $a, c \in P$.

(b) Bezeichne (bei festem $a \in P, j \in I, i \neq j$) die Zahl der $c \in P$ mit $\mu_{ij}(a, c) > 0$ mit t. Wegen (SBTS2) ist $t \leqslant v - 1$. Wegen $\mu(v-1) = \rho_i(a) = \sum_{c \in P} \mu_{ij}(a, c) = t\mu_{ij}$ ist $\mu_{ij} \mid t\mu_{ij} = \mu(v-1) \leqslant (v-1)\mu_{ij}$, mit Gleichheit genau dann, wenn $\mu_{ij}(a, c) > 0$ für alle $c \neq a$; d.h. wegen (SBTS3), wenn $\mu_{ij}(a, c) = \mu_{ij} = \mu$ für alle $c \neq a$.

Wenn wir so für alle $a \in P$, $i, j \in I$, $i \neq j$ verfahren, erhalten wir (2), und Gleichheit gilt genau dann, wenn $\mu_{ij}(a, c) = \mu$ für alle $c \neq a$, d.h. wenn (SBTS3a) erfüllt ist. Umgekehrt folgt wegen $\rho_i(a) = \sum_{c \in P} \mu_{ij}(a, c) = \sum_{c \neq a} \mu = \mu(v-1)$ (SBTS3) aus (SBTS3a) (mit $\mu_{ij} = \mu$ für alle $i \neq j$).

(c) Ist $\alpha \in G$, $\alpha x = x$, so ist $x_i = x_{\alpha i}$ füralle i, und wegen (SBST2) daher $\alpha i = i$ für alle i, d.h. $\alpha = 1$. Also ist $\alpha x \neq x$ für $\alpha \in G - \{1\}$. Der Stabilisator G_{ij} zerlegt daher Q in Bahnen der Länge $|G_{ij}|$. Da mit $x_i = a$, $x_j = c$ auch $y_i = a$, $y_j = c$ für alle y in der G_{ij}-Bahn von x ist, ist $|G_{ij}|$ ein Teiler von $\mu_{ij}(a, c) \in \{0, \mu_{ij}\}$, also $|G_{ij}| \mid \mu_{ij}$ (bei geeigneter Wahl von c). (Dieses Argument ist nicht anwendbar, falls $Q = \emptyset$; aber dann ist nach (SBTS3) $v = 1$ oder $\mu = 0$, was wir ausgeschlossen haben.)

Analog zerlegt G_i Q in Bahnen der Länge $|G_i|$, und $|G_i| \mid \rho_i(a) = \mu(v-1)$. Schließlich zerlegt G Q in Bahnen der Länge $|G|$, also ist $|G| \mid b = \mu v(v-1)$.

2.2.3. *Definition* (*einfache SBTS*). Ein $(v, k, \mu, M; G)$-SBTS heißt einfach, wenn $\mu_{ij} = |G_{ij}|$ für alle $i, j \in I$, $i \neq j$ und $\mu = \min_{\substack{i, j \in I \\ i \neq j}} |G_{ij}|$.

Diese Definition ist wegen 2.2.2 sinnvoll. Die einfachen SBTS sind neben den $(v, k, \mu; G)$-SBTS die wichtigsten Spezialfälle. Beachte, daß die

Gruppe G die Parameter μ und M des einfachen SBTS eindeutig festlegt. Einfache SBTS mit $k = 3, 4$ behandeln wir in Kapitel 6.

2.2.4. *Beispiel.* K sei der endliche Körper $GF(q)$, e sei Teiler von $q - 1$, und H^e sei die Gruppe der e-ten Potenzen in K. Dann ist $Q = \{(ia + b : i \in H^e) \mid a, b \in K, a \neq 0\}$ ein (einfaches) $\left(q, \frac{q-1}{e}; H^e\right)$-SBTS über K. H^e operiert dabei auf den Stellen durch Multiplikation. Wir übergehen den einfachen Beweis.

2.2.5. *Definition (Homogenes Tupelsystem, HTS).* Ein $(v, k, \mu; G)$-HTS ist ein (v, k)-Tupelsystem (P, I, Q, ϵ) mit den Eigenschaften

(HTS1) G ist Gruppe freier Automorphismen von (P, I, Q, ϵ),

(HTS2) $\mu_{ij}(a, c) = \mu$ für alle $a, c \in P, i, j \in I, i \neq j$.

Wir nennen ein $(v, k, \mu; G)$-HTS primär, wenn $\mu = 1$, maximal, wenn $k = \frac{v^2\mu - 1}{v - 1}$, und idempotent, wenn gilt: $x_{i_1} = x_{i_2} = a, i_1 \neq i_2 \Rightarrow x_i = a$ für alle $i \in I$.

Ist G trivial, so lassen wir G von der Parametreliste weg. Die Bezeichnung maximales HTS für $k = \frac{v^2\mu - 1}{v - 1}$ erklärt sich aus der in Satz 2.2.10 bewiesenen Ungleichung $k \leqslant \frac{v^2\mu - 1}{v - 1}$ für alle (v, k, μ)-HTS mit $v > 1$.

2.2.6. *Definition (Transversale).* (P, I, Q, ϵ) sei ein (v, k)-Tupelsystem. Eine Teilmultimenge T von Q heißt ρ-Transversale von Q, wenn $\rho_i^T(a) = \rho$ für alle $a \in P, i \in I$. Statt 1-Transversale sagen wir einfach Transversale.

Es gibt einen fast trivialen, aber bemerkenswerten Zusammenhang zwischen idempotenten $(v, k, \mu; G)$-HTS und $(v, k, \mu; G)$-SBTS:

2.2.7. *Satz.* (a) Q sei ein $(v, k, \mu; G)$-SBTS über P. Dann ist das Tupelsystem $Q' = Q \cup \mu \times \{(a, \ldots, a) \mid a \in P\}$ ein idempotentes $(v, k, \mu; G)$-HTS.

(b) Q' sei ein idempotentes $(v, k, \mu; G)$-HTS über P. Dann enthält Q' jedes Tupel $(a, \ldots, a)$, $a \in P$ genau μ-mal, $T = \mu \times \{(a, \ldots, a) \mid a \in P\}$ ist eine μ-Transversale von Q', und $Q = Q' - T$ ist ein $(v, k, \mu; G)$-SBTS.

Beweis. (a) ist trivial. (b) Wir können o.B.d.A. $k \geqslant 2$ annehmen. Es gibt genau μ Tupel $x \in Q'$ mit $x_1 = x_2 = a$, die wegen der Idempotenz von Q' alle die Form $(a, \ldots, a)$ haben. Insbesondere ist T eine Teilmultimenge von Q', und offensichtlich eine μ-Transversale. Ist nun $x \in Q'$ ein Tupel mit zwei gleichen Einträgen $x_i = x_j = a, i \neq j$, so ist wegen der Idempotenz auch $x_1 = x_2 = a$, und daher $x \in T$. Also ist $\mu_{ij}^Q(a, a) = 0$

für alle $a \in P$, $i, j \in I$, $i \neq j$. (SBTS1) und (SBTS3a) folgen sofort aus (HTS1) und (HTS2).

Die Begriffe HTS und Transversale sind invariant unter Isotopismen. Jedoch bleibt die Gruppe G der freien Automorphismen i.A. nur bei Isomorphismen erhalten (die Bildgruppe ist dann $\alpha G \alpha^{-1}$).

Wir bemerken, daß sich die Situationszahlen eines (v, k, μ)-HTS aus (HTS2) ergeben: $\rho_i(a) = \sum_{c \in P} \mu_{ij}(a, c) = |P| \mu = \mu v$, $b = \sum_{a \in P} \rho_i(a) = |P| \mu v = \mu v^2$.

Als Beispiel eines primitiven HTS haben wir schon in 2.1.5 ein $(v, 3, 1; S_3)$-HTS angegeben. Dieses HTS ist idempotent, wenn K eine elementar abelsche 3-Gruppe ist.

2.2.8. *Proposition.* Ein (v, k, μ)-HTS Q ist genau dann zu einem idempotenten HTS isotop, wenn Q eine μ-Transversale enthält, die das μ-fache einer Transversale von Q ist. Insbesondere ist jedes primitive HTS, das eine Transversale besitzt, zu einem idempotenten primitiven HTS isotop.

Denn die Eigenschaft, μ-Transversale zu sein, ist Isotopie invariant, also enthält nach 2.2.7*b*) jedes zu einem idempotenten HTS isotope Tupelsystem eine μ-Transversale der geforderten Art. Ist umgekehrt T eine Transversale von Q mit $\mu \times T \subseteq Q$, so ist $T = \{(\pi_i a : i \in I) \mid a \in P\}$ mit Abbildungen π_i, die wegen $\rho_i^T(a) = 1$ Permutationen sind. Der Isotopismus $(\pi_i^{-1} : i \in I)$ bildet daher Q auf ein idempotentes HTS ab.

Wir erwähnen noch ein wichtiges Reduktionsprinzip, dessen Beweis wieder trivial ist:

2.2.9. (P, I, Q, ϵ) sei ein (v, k, μ)-HTS. Ist dann I_0 eine k_0-Teilmenge von I, so ist $(P, I_0, Q, \epsilon|_{Q \times I_0})$ ein (v, k_0, μ)-HTS.

In Multimengenschreibweise: Ist Q ein (v, k, μ)-HTS über P, so ist für eine k_0-Teilmenge I_0 von I das Tupelsystem $Q|^{I_0} = \{(x_i : i \in I_0) \mid x \in Q\}$ ein (v, k_0, μ)-HTS.

2.2.10. *Satz.* (P, I, Q, ϵ) sei ein (v, k, μ)-HTS. Dann gilt

$$k \leqslant \frac{v^2\mu - 1}{v - 1} \text{ für } v > 1, \mu > 0. \tag{4}$$

Gleichheit gilt genau dann, wenn die folgende Bedingung erfüllt ist:

(R) Für alle $x, y \in Q$, $x \neq y$ gibt es genau λ Stellen $i \in I$ mit $x_i = y_i$.

Es ist dann $\lambda = \frac{v\mu - 1}{v - 1}$.

Beweis. Wir führen den Beweis unter Verwendung der im nächsten Abschnitt eingeführten PBD (Def. 2.3.1).

$z \in Q$ sei ein beliebiges Tupel. Mit $B_z(x) = \{i \in I \mid x_i = z_i\}$ $(x \in Q)$ und $\mathcal{B}_z = \{B_z(x) \mid x \in Q, x \neq z\}$ ist dann $(I, \mathcal{B}_z)$ ein reguläres PBD vom Index $\lambda' = \mu_{ij}(z_i, z_j) - 1 = \mu - 1$ mit $v' = k$ Punkten, $b' = v^2\mu - 1$ Blöcken, $r' = \rho_i(z_i) - 1 = v\mu - 1$ Blöcken durch jeden Punkt. Anwendung von Proposition 2.3.8. liefert $v^2\mu - 1 \geqslant \dfrac{(v\mu - 1)^2 k}{(v\mu - 1) + (\mu - 1)(k - 1)}$, und nach Vereinfachung ergibt sich (4). Gleichheit gilt genau dann, wenn alle Blöcke $B_z(x)$ gleiche Länge haben, die dann gleich $\dfrac{r'v'}{b'} = \dfrac{(v\mu - 1)k}{v^2 - 1} = \dfrac{v\mu - 1}{v - 1}$ ist. Daraus ergibt sich der Rest des Satzes.

2.3. Andere Strukturen

In diesem Abschnitt geben wir einige später benötigte Definitionen und Sätze (ohne Beweis) aus der Theorie der Blockpläne an.

2.3.1. *Definition (pairwise balanced design, PBD).* Ein (v, K, λ)-PBD ist ein Paar $(P, \mathcal{B})$ bestehend aus einer v-Menge P von "Punkten" und einer Multimenge $\mathcal{B}$ von Teilmengen von P ("Blöcken") mit den Eigenschaften

(PBD1) Jedes Paar verschiedener Punkte liegt in genau λ Blöcken von $\mathcal{B}$,

(PBD2) $|B| \in K$ für alle $B \in \mathcal{B}$.

Das PBD heißt regulär (mit Parameter r), wenn gilt:

(PBD3) Jeder Punkt liegt in genau r Blöcken von $\mathcal{B}$.

Statt "$(P, \mathcal{B})$ ist (v, K, λ)-PBD" sagen wir auch "$(P, \mathcal{B})$ ist ein PBD vom Index λ mit Blocklängen aus K".

Eine Parallelklasse eines PBD ist eine Menge $\mathcal{G}$ von Blöcken derart, daß jeder Punkt in genau einem Block von $\mathcal{G}$ liegt.

2.3.2. *Definition (Blockplan = balanced incomplete block design, BIBD).* Ein (v, k, λ)-Blockplan ist ein PBD vom Index λ mit Blocklängen aus $\{k\}$, d.h. also ein PBD, in dem jeder Block genau k Punkte enthält.

Zur Theorie der Blockpläne und PBD, insbesondere für die Beweise der folgenden Aussagen, siehe etwa Hall [9], Ryser [22], Raghavarao [21], Dembowski [5], Hanani [10], [11], Wilson [28], [29], [30].

2.3.3. *Satz.* Die auf den Teilmengen der Menge der natürlichen Zahlen durch $B(K) = \{v \mid$ Es existiert ein $(v, K, 1)$-PBD$\}$ definierte Operation B ist eine Hüllenoperation, d.h. es gilt

(H1) $K \subseteq B(K)$,

(H2) $L \subseteq K \Rightarrow B(L) \subseteq B(K)$,

(H3) $B(B(K)) = B(K)$.

2.3.4. *Definition* (*PBD-abgeschlossen*). Eine Menge K natürlicher Zahlen heißt PBD-abgeschlossen, wenn $B(K) = K$, d.h., wenn gilt:

(A) Ist $(P, \mathcal{B})$ ein PBD vom Index 1, und $|B| \in K$ für alle $B \in K$, so ist $|P| \in K$.

Nennen wir eine Teilmenge K einer Menge N eine kofinale Teilmenge von N, falls N-K endlich ist, so gilt.

2.3.5. *Satz* (*Wilson*). Jede PBD-abgeschlossene Menge $K \neq \emptyset, \{1\}$ ist eine kofinale Teilmenge der Menge

$$H_\beta^\alpha = \{v \in \mathbb{N} \mid \alpha | v - 1, \quad \beta | v(v-1)\},$$

wo die Zahlen α, β gegeben sind durch

$$\alpha = \operatorname*{ggT}_{v \in K} (v - 1), \quad \beta = \operatorname*{ggT}_{v \in K} (v(v-1)). \tag{1}$$

(Dabei bedeutet ggT den größten gemeinsamen Teiler der nachstehenden Elemente.)

2.3.6. *Proposition.* Ist $(P, \mathcal{B})$ ein PBD vom Index λ, so gelten die Gleichungen

$$\sum_{a \in B \in \mathcal{B}} (|B| - 1) = \lambda(|P| - 1) \text{ für alle } a \in P, \tag{2}$$

$$\sum_{B \in \mathcal{B}} |B| (|B| - 1) = \lambda |P| (|P| - 1). \tag{3}$$

Insbesondere ist für (v, k, λ)-Blockpläne $r = \dfrac{\lambda(v-1)}{k-1}$ die Zahl der Blöcke, die einen festen Punkt enthalten, und $b = \dfrac{\lambda v(v-1)}{k(k-1)}$ die Zahl der Blöcke überhaupt.

2.3.7. *Satz.* $(P, \mathcal{B})$ sei ein (v, k, λ)-Blockplan.

(a) Ist $v > k$, so ist $b \geqslant v$ (Fisher-Ungleichung).

(b) Ist $b = v$, so haben je zwei Blöcke genau λ gemeinsame Punkte. Außerdem gilt mit $n = r - \lambda$ (Bruck-Ryser-Bedingung):

(i) ist v gerade, so ist n eine Quadratzahl,

(ii) ist v ungerade, so hat die diophantische Gleichung $nx^2 + (-1)^{\frac{v-1}{2}} vy^2 = z^2$ eine nichttriviale ganzzahlige Lösung.

2.3.8. *Proposition.* $(P, \mathcal{B})$ sei ein reguläres (v, K, λ)-PBD mit b Blöcken und r Blöcken durch jeden Punkt. Dann ist

$$b \geqslant \frac{r^2 v}{r + \lambda(v-1)} \tag{4}$$

und Gleichheit gilt genau dann, wenn $(P, \mathcal{B})$ ein (v, k, λ)-Blockplan ist $\left(\text{mit } k = \frac{rv}{b}\right)$.

Da ich in der Literatur keinen Beweis dafür kenne, gebe ich einen an. Aus den Gleichungen $\sum_{B\in\mathcal{B}} 1 = b$, $\sum_{B\in\mathcal{B}} |B| = \sum_{B\in\mathcal{B}} \sum_{a\in\mathcal{B}} 1 = \sum_{a\in P} \sum_{a\in B\in\mathcal{B}} 1$ $= vr$ ergibt sich mit (3)

$$0 \leqslant \sum_{B\in\mathcal{B}} \left(|B| - \frac{rv}{b}\right)^2 = \frac{bv(r + \lambda(v-1)) - r^2v^2}{b},$$

und (4) ergibt sich unmittelbar. Gleichheit gilt in (4) genau dann, wenn die angegebene Quadratsumme Null wird, also wenn $|B| = \frac{rv}{b}$ ist für alle $B \in \mathcal{B}$.

3. ÄQUIVALENTE KOMBINATORISCHE STRUKTUREN

Dieses Kapitel stellt den Zusammenhang zwischen Tupelsystemen und anderen kombinatorischen Strukturen her. Es ergeben sich eine Vielzahl von Verknüpfungen mit diesen.

In Abschnitt 3.1. behandeln wir eine Verallgemeinerung der Transversalpläne und beweisen ihre Aquivalenz zu Tupelsystemen. Als Spezialfall ergibt sich die Äquivalenz von Transversalplänen und HTS.

Strukturen, in denen das Euklidische Parallelenaxiom gilt (verallgemeinerte Netze), werden in Abschnitt 3.2. untersucht. Eine Äquivalenz zwischen verallgemeinerten Netzen und Tupelsystemen wird aus einer Dualität zu verallgemeinerten Transversalplänen hergeleitet. Diese Äquivalenz wird benutzt, um einerseits Netze durch HTS zu charakterisieren, andrerseits auflösbare (resolvable) Blockpläne als Tupelsysteme darzustellen. Außerdem ergibt sich eine Charakterisierung von affinen (affine resolvable) Blockplänen durch maximale HTS.

Die Äquivalenz von HTS mit orthogonalen Arrays wird in Abschnitt 3.3. festgestellt. Ebenfalls behandelt wird die Darstellung durch paarweise orthogonale Lateinische Quadrate bzw. Quasigruppen. Satz 3.3.6. faßt alle sieben äquivalente Beschreibungen für $(v, k, 1)$-HTS zusammen.

Beziehungen zwischen SBTS und Blockplänen behandelt Abschnitt 3.4. Dort wird zu jedem $(v, k, \mu; G)$-SBTS ein Blockplan konstruiert, und umgekehrt erhält man aus einem Blockplan solche SBTS für zweifach transitive freie Automorphismengruppen. Als Folgerung werden weitere Existenzkriterien für SBTS bewiesen.

Abschnitt 3.5. zeigt schließlich die Äquivalenz von Roomschen Quadraten mit einer gewissen Klasse von SBTS.

3.1. Verallgemeinerte Transversalpläne

3.1.1. *Definition* (*Transversalplan, GTD*). Ein verallgemeinerter Transversalplan (generalized transversal design, GTD) ist ein Tripel $J = (X, \mathcal{G}, \mathcal{B})$, bestehend aus einer vk-Menge X von "Punkten", einer Partition $\mathcal{G}$ von X in k "Gruppen" zu je v Punkten, und einer Multimenge $\mathcal{B}$ von Teilmengen von X ("Blöcke") mit der Eigenschaft

(TD1) Jede Gruppe hat mit jedem Block genau einen Punkt gemeinsam.

Das GTD heißt ein Transversalplan (transversal design, TD), genauer ein $(k, \mu; v)$-TD, wenn außerdem gilt:

(TD2) Für jede Wahl von Punkten a, b aus verschiedenen Gruppen gibt es genau μ Blöcke, die a und b enthalten.

Eine unmittelbare Folgerung aus (TD1) ist.

3.1.2. Jeder Block eines GTD enthält genau k Punkte.

3.1.3. *Definition* (*group divisible design, GDD*). Ein $(k, \mu, m; v)$-GDD ist ein Tripel $J = (X, \mathcal{G}, \mathcal{B})$, bestehend aus einer v-Menge X von "Punkten", einer Partition $\mathcal{G}$ von X in "Gruppen" der Länge m, und einer Multimenge $\mathcal{B}$ von k-Teilmengen von X ("Blöcken") mit den Eigenschaften

(GDD1) Liegen a, b in verschiedenen Gruppen, so gibt es genau μ Blöcke, die a und b enthalten,

(GDD2) Liegen a und b $(a \neq b)$ in derselben Gruppe, so gibt es keinen Block, der a und b enthält.

3.1.4. *Proposition.* Jedes $(k, \mu; v)$-TD ist ein $(k, \mu, v; vk)$-GDD und umgekehrt.

Beweis. (a) J sei ein $(k, \mu; v)$-TD. (TD2) ist gerade Bedingung (GDD1), und aus (TD1) ergibt sich sofort (GDD2). Ein Anzahlvergleich zeigt nun, daß J ein $(k, \mu, v; vk)$-GDD ist.

(b) $J = (X, \mathcal{G}, \mathcal{B})$ sei ein $(k, \mu, v; vk)$-GDD. (GDD1) ergibt (TD2). $\mathcal{G}$ ist Partition der vk-Menge X in v-Mengen, also enthält $\mathcal{G}$ genau k Gruppen. Wegen (GDD2) genügt es nun zu zeigen, daß jeder Block mit jeder Gruppe mindestens einen Punkt gemeinsam hat. Angenommen, es wäre $A_0 \in \mathcal{G}$, $B_0 \in \mathcal{B}$ mit $A_0 \cap B_0 = \emptyset$. Das ergibt den Widerpruch

$$k = |B_0| = \sum_{A \in \mathcal{G}} |A \cap B_0| \leqslant \sum_{A \in \mathcal{G} - \{A_0\}} 1 = k - 1.$$

Daher ist J ein $(k, \mu; v)$-TD.

Über weitere Eigenschaften und über die Verwendung von Transversalplänen und GDD siehe die Literaturangaben nach Definition 2.3.2., insbesondere die Arbeiten von Hanani und Wilson.

3.1.5. *Definition* (*Isomorphie*). Ein Isomorphismus eines GTD $J = (X, \mathcal{G}, \mathcal{B})$ auf das GTD $J' = (X', \mathcal{G}', \mathcal{B}')$ ist ein Tripel (ρ, σ, τ) von Bijektionen $\rho : X \to X'$, $\sigma : \mathcal{G} \to \mathcal{G}'$, $\tau : \mathcal{B} \to \mathcal{B}'$ derart, daß für alle $a \in X$ und alle $A \in \mathcal{G}$, $B \in \mathcal{B}$ gilt:

$$a \in A \to \rho a \in \sigma A; \quad a \in B \to \rho a \in \tau B. \tag{1}$$

J und J' heißen isomorph, wenn ein Isomorphismus von J auf J' existiert.

Man bestätigt ohne weiteres:

3.1.6. Die Isomorphie von GTD ist eine Äquivalenzrelation.

Ein GTD, das nur (TD1) erfüllt, ist i.A. ziemlich strukturlos. Das wird sofort deutlich aus dem folgenden.

3.1.7. *Äquivalenzsatz für GTD.* Die Klassen isomorpher GTD entsprechen eineindeutig den Klassen isotoper Tupelsysteme bei der folgenden Zuordnung:

(a) Ist (P, I, Q, ϵ) ein (v, k)-Tupelsystem, so ist

$J = (P \times I, \{P \times \{i\} \mid i \in I\}, \{B_x \mid x \in Q\})$ mit $B_x = \{(x_i, i) \mid i \in I\} (x \in G)$

ein GTD.

(b) $J = (X, \mathcal{G}, \mathcal{B})$ sei ein GTD mit k Gruppen der Länge v. P sei eine v-Menge, und die Punkte jeder Gruppe $A \in \mathcal{G}$ seien numeriert als $p(A, a)$, $a \in P$. Dann ist das Quadrupel $(P, \mathcal{G}, \mathcal{B}, \epsilon)$ ein Tupelsystem mit der durch "$p(A, \epsilon(B, A))$ ist der A und B gemeinsame Punkt" definierten Belegung ϵ. Die Konstruktion ist (bis auf Isomorphie) invers zu (*a*).

Beweis. Daß bei (a), (b) wirklich ein GTD bzw. ein Tupelsystem entsteht, ist klar.

Numeriert man die Gruppen $P \times \{i\}$ des in (*a*) konstruierten GTD als $p(P \times \{i\}, a) = (a, i)$, so erhält man durch (b) offensichtlich ein isotopes Tupelsystem $(\alpha i = P \times \{i\}, \pi a = a, \phi x = B_x)$. Daher sind die Konstruktionen zueinander invers, und es genügt zu zeigen, daß isotope Tupelsysteme in isomorphe GTD übergeführt werden, und umgekehrt.

(a) (α, π) sei ein Isotopismus des Tupelsystems (P, I, Q, ϵ) auf (P', I', Q', ϵ'), und ϕ eine zugehörige Bijektion $Q \to Q'$. Setzt man $\rho : (a, i) \to (\pi_i a, \alpha i)$, $\sigma : P \times \{i\} \to P' \times \{\alpha i\}$, $\tau : B_x \to B_{\phi x}$, so gilt $(a, i) \in P \times \{j\} \Leftrightarrow i = j \Leftrightarrow \rho(a, i) = (\pi_i a, \alpha i) \in P' \times \{\alpha i\} = \sigma(P \times \{i\} = \sigma(P \times \{j\})$, und $(a, i) \in B_x \Leftrightarrow x_i = a \Leftrightarrow (\phi x)_{\alpha i} = \pi_i a \Leftrightarrow \rho(a, i) = (\pi_i a, \alpha i) \in B_{\phi x} = \tau B_x$. Daher ist (ρ, σ, τ) ein Isomorphismus der zugehörigen GTD.

(b) (ρ, σ, τ) sei ein Isomorphismus des GTD $(X, \mathcal{G}, \mathcal{B})$ auf das GTD $(X', \mathcal{G}', \mathcal{B}')$. Wie in der Konstruktion sei $A = \{p(A, a) \mid a \in P\}$ für $A \in \mathcal{G}$, $A' = \{p'(A', a) \mid a \in P'\}$ für $A' \in \mathcal{G}'$ die Numerierung der Punkte in den Gruppen. Es ist $p(A, a) \in A$, also $\rho(p(A, a)) \in \sigma A$, und daher $\rho(p(A, a)) =$

$p'(\sigma A, \pi_A a)$ für eine Abbildung $\pi_A : P \to P'$, die sich sofort als Bijektion erweist. (σ, π) mit $\pi = (\pi_A : A \in \mathcal{G})$ ist der gesuchte Isotopismus von $(P, \mathcal{G}, \mathcal{B}, \epsilon)$ auf $(P', \mathcal{G}', \mathcal{B}', \epsilon')$. Denn $\epsilon(B, A) = a \Leftrightarrow p(A, a) \in A \cap B \Rightarrow p'(\sigma A, \pi_A a) = \rho(p(A, a)) \in \sigma A \cap \tau B \Rightarrow \epsilon'(\tau B, \sigma A) = \pi_A a$, was die Behauptung beweist.

3.1.8. *Äquivalenzsatz für TD.* Die Klassen isomorpher $(k, \mu; v)$-TD und die Klassen isotoper (v, k, μ)-HTS entsprechen sich bei der in 3.1.7. angegebenen Konstruktion eineindeutig.

Beweis. (P, I, Q, ϵ) sei ein (v, k)-Tupelsystem, und J das zugehörige GTD. Die Zahl der Blöcke, die (a, i) und (b, j) $(i \neq j)$ enthalten, ist gleich der Zahl der Tupel $x \in Q$ mit $x_i = a$, $x_j = b$, also $= \mu_{ij}(a, b)$. Daher ist J ein $(k, \mu; v)$-TD genau dann, wenn $\mu_{ij}(a, b) = \mu$ für alle $i \neq j$ und alle a, b, d.h. genau dann, wenn Q ein (v, k, μ)-HTS ist.

3.2. Verallgemeinerte Netze. Auflösbarer Blockplane

3.2.1. *Definition (verallgemeinertes Netz).* Ein verallgemeinertes Netz ist ein Tripel $\mathcal{N} = (X, \mathcal{B}, \|)$, mit einer endlichen Menge X von "Punkten", einer Multimenge $\mathcal{B}$ von Teilmengen von X ("Blöcken") und einer Äquivalenzrelation $\|$ von $\mathcal{B}$ ("Parallelismus") mit k Parallelklassen zu je v Blöcken, derart daß gilt:

(NET1) Für jeden Punkt $a \in X$ und jeden Block $B \in \mathcal{B}$ gibt es genau einen Block $C \| B$ mit $x \in C$. ("Euklidisches Parallelenaxiom") Gilt außerdem

(NET2) Je zwei nichtparallele Blöcke haben genau μ gemeinsame Punkte, so heißt $\mathcal{N}$ ein (v, k, μ)-Netz (oder k-Netz, falls $\mu = 1$).

Offensichtlich gilt:

3.2.2. Jeder Punkt eines verallgemeinerten Netzes liegt auf genau k Blöcken.

3.2.3. *Definition (auflösbarer (= resolvable) Blockplan, RBIBD).* Ein verallgemeinertes Netz $(X, \mathcal{B}, \|)$ heißt RBIBD, wenn $(X, \mathcal{B})$ ein Blockplan ist. Ist $(X, \mathcal{B}, \|)$ sogar ein Netz, so heißt der Blockplan affin (ARBIBD).

3.2.4. *Definition (Isomorphie).* Ein Isomorphismus des verallgemeinerten Netzes $\mathcal{N} = (X, \mathcal{B}, \|)$ auf $\mathcal{N}' = (X', \mathcal{B}', \|')$ ist ein Paar (ρ, τ) von Bijektionen $\rho : X \to X'$, $\tau : \mathcal{B} \to \mathcal{B}'$ mit

$$a \in B \to \rho a \in \tau B; \quad B \| C \to \tau B \| \tau C. \tag{1}$$

Zwei verallgemeinerte Netze $\mathcal{N}$, $\mathcal{N}'$ sind isomorph, wenn ein Isomorphismus von $\mathcal{N}$ nach $\mathcal{N}'$ existiert.

3.2.5. Die Isomorphie von Netzen ist eine Äquivalenzrelation.

Zwischen verallgemeinerten Netzen und verallgemeinerten Transversalplänen besteht der folgende Zusammenhang:

3.2.6. *Dualitätssatz.* (a) Ist $J = (X, \mathcal{G}, \mathcal{B})$ ein GTD, so ist $(\mathcal{B}, \{B_a \mid a \in X\}, \|)$ mit $B_a = \{B \mid a \in B \in \mathcal{B}\}$, $B_a \| B_b \Leftrightarrow a, b$ liegen in derselben Gruppe, ein verallgemeinertes Netz.

(b) Ist $\mathcal{N} = (X, \mathcal{B}, \|)$ ein verallgemeinertes Netz, so ist $J = (\mathcal{B}, \mathcal{G}, \{B_a \mid a \in x\})$, wo $B_a = \{B \mid a \in B \in \mathcal{B}\}$, und $\mathcal{G}$ die durch $\|$ induzierte Klasseneinteilung von $\mathcal{B}$ ist, ein GTD.

(c) Die Konstruktionen (a) und (b) induzieren eine eineindeutige Zuordnung zwischen den Klassen isomorpher GTD und den Klassen isomorpher verallgemeinerter Netze.

(d) Das einem GTD nach (a) zugeordnete verallgemeinerte Netz ist genau dann ein (v, k, μ)-Netz, wenn das GTD ein $(k, \mu; v)$-TD ist.

Der einfache Beweis kann dem Leser überlassen werden.

Aus dem Äquivalenzsatz für GTD (3.1.7) ergibt sich nun leicht:

3.2.7. *Äquivalenzsatz für verallgemeinerte Netze.* Die Klassen isomorpher verallgemeinerter Netze und die Klassen isotoper Tupelsysteme entsprechen sich eineindeutig bei der folgenden Zuordnung:

(a) Ist (P, I, Q, ϵ) ein Tupelsystem, so ist mit $B_{i,a} = \{x \in Q \mid x_i = a\}$, $B_{i,a} \| B_{j,b} \Leftrightarrow i = j$ das Tripel $\mathcal{N} = (Q, \{B_{i,a} \mid i \in I, a \in P\}, \|)$ ein verallgemeinertes Netz.

(b) $(X, \mathcal{B}, \|)$ sei ein verallgemeinertes Netz mit Parallelklassen der Länge v. I sei eine Indexmenge für die Parallelklassen, P sei eine v-Menge, und die Blöcke der i-ten Parallelklasse ($i \in I$) seien $B_{i,a}$ ($a \in P$). Dann ist (P, I, X, ϵ) mit $\epsilon(x, i) = a \Leftrightarrow x \in B_{i,a}$ ($\Leftrightarrow$ der x enthaltende Block der i-ten Parallelklasse ist $B_{i,a}$) ein Tupelsystem. Die Konstruktion ist invers zu a).

3.2.8. *Satz.* (P, I, Q, ϵ) sei ein Tupelsystem, und $\mathcal{N}$ sei das nach 3.2.7. zugehörige verallgemeinerte Netz.

(a) $\mathcal{N}$ ist genau dann ein (v, k, μ)-Netz, wenn Q ein (v, k, μ)-HTS ist.

(b) $\mathcal{N}$ ist genau dann RBIBD, wenn Q die folgenden Bedingungen erfüllt:

(R1) $\rho_i(a) = \rho$ für alle $a \in P$, $i \in I$,

(R2) Für alle $x, y \in Q$, $x \neq y$ gibt es genau λ' Stellen $i \in I$ mit $x_i = y_i$. In diesem Fall hat das RBIBD die Parameter

$$v' = v\rho,\ k' = \rho,\ b' = vk,\ r' = k,\ \lambda' = \frac{k(\rho - 1)}{v\rho - 1}. \qquad (2)$$

(c) $\mathcal{N}$ ist genau dann ARBIBD, wenn Q ein (v, k, μ)-HTS mit $k = \dfrac{v^2\mu - 1}{v - 1}$ ist. Das ARBIBD hat dann die Parameter

$$v' = v^2\mu,\ k' = v\mu,\ b' = v\,\frac{v^2\mu - 1}{v - 1},\ r' = \frac{v^2\mu - 1}{v - 1},\ \lambda' = \frac{v\mu - 1}{v - 1}. \qquad (3)$$

Beweis. (a) Die Zahl der gemeinsamen Punkte der nichtparallelen Blöcke $B_{i,a}$ und $B_{j,b}$ $(i \neq j)$ ist gleich $\mu_{ij}(a, b)$. Daraus ergibt sich unmittelbar (a).

(b) Jeder Punkt x von $\mathcal{N}$ liegt auf genau $r' = k$ Blöcken $B_{i,a}$. Also ist $\mathcal{N}$ genau dann RBIBD, wenn (i) jeder Block $B_{i,a}$ enthält genau k' Punkte, d.h. $\rho_i(a) = k' = \rho$ unabhängig von i, a, und (ii) je zwei Punkte $x \neq y$ liegen auf genau λ' Blöcken $B_{i,a}$, d.h. $x_i = y_i\ (=a)$ für genau λ' Stellen $i \in I$. Daher gelten (R1) und (R2) genau dann, wenn $\mathcal{N}$ RBIBD ist. Die Parameter (2) ergeben sich nun aus $v' = v\rho$ (Folge von (R1)), $b' = vk$ (klar), $r' = k$ und den Gleichungen $b'k'(k' - 1) = v'(v' - 1)$ und $r'(k' - 1) = \lambda'(v' - 1)$, die in jedem Blockplan gelten (Proposition 2.3.6).

(c) $\mathcal{N}$ ist genau dann ARBIBD, wenn es Netz und RBIBD ist, also wenn Q ein (v, k, μ)-HTS ist und (R1), (R2) gelten. Aber (R2) gilt in jedem (v, k, μ)-HTS mit $\rho = v\mu$, und (R2) ist nach Satz 2.2.10 genau dann erfüllt, wenn $k = \dfrac{v^2\mu - 1}{v - 1}$, $\lambda' = \dfrac{v\mu - 1}{v - 1}$ ist. Die Parameter (3) ergeben sich daraus mit (2).

Bemerkung. Wir nennen ein ARBIBD mit den Parametern (3) ein (μ, v)-ARBIBD. Ein $(1, v)$-ARBIBD ist eine affine Ebene der Ordnung v; also entsprechen sich Klassen isomorpher affiner Ebenen und Klassen isotoper $(v, v + 1, 1)$-HTS eineindeutig. Siehe dazu, und für Anwendungen auf affine Ebenen, Neumaier [18].

3.3. Orthogonale Arrays, Lateinische Quadrate und Quasigruppen

3.3.1. *Definition (Orthogonale Array, OA).* Eine (N, k, s, t)-OA vom Index λ ist eine $k \times N$-Matrix A mit Einträgen aus einer s-Menge, mit der Eigenschaft

(OA1) Jede $t \times N$-Untermatrix von A enthält alle möglichen $t \times 1$-Spaltenvektoren mit derselben Häufigkeit λ. Offensichtlich gilt:

3.3.2. *Proposition.* (a) Für eine (N, k, s, t)-OA vom Index λ gilt $N = \lambda s^t$.

(b) eine (N, k, s, t)-OA vom Index λ ist auch eine (N, k, s, t')-OA vom Index $\lambda s^{t-t'}$, für alle $t' \leqslant t$.

3.3.3. *Äquivalenzsatz für Orthogonale Arrays.* (a) (P, I, Q, ϵ) sei ein

(v, k, μ)-HTS. Numeriert man die Tupel von Q als $x^{(1)}, \ldots, x^{(v^2\mu)}$, so ist die Matrix $A = (a_{ij})_{j=1, \ldots, v^2\mu}^{i=1, \ldots, k}$ mit $a_{ij} = x_i^{(j)}$ eine $(v^2\mu, k, v, 2)$-OA vom Index μ.

(b) $A = (a_{ij})$ sei eine $(v^2\mu, k, v, 2)$-OA vom Index μ. Dann ist das Tupelsystem $Q = (a_{1j}, \ldots, a_{kj})$ $j = 1, \ldots, v^2\mu$ ein (v, k, μ)-HTS.

Beweis. Trivial.

3.3.4. *Definition* (*Lateinisches Quadrat*). Ein Lateinisches Quadrat der Ordnung v (über der v-Menge P) ist eine $v \times v$-Matrix A mit Einträgen aus P mit

(L1) Jede Zeile und jede Spalte von A enthält jedes Element von P genau einmal.

Zwei Lateinische Quadrate $A = (a_{ij})$, $B = (b_{ij})$ über P heißen orthogonal, wenn

(L2) Jedes Paar $(a, b) \in P \times P$ tritt genau einmal als (a_{ij}, b_{ij}), $i, j = 1, \ldots, v$, auf.

Ein Lateinisches Quadrat A, das zu A^T orthogonal ist, heißt selbstorthogonal (Dabei ist A^T die Transponierte von A).

3.3.5. *Definition* (*Quasigruppe*). Eine Quasigruppe (auf P) ist ein Paar $(P, *)$ wo $*$ eine binäre Operation auf P, die die Kürzungsregeln $(a * x = a * y \Rightarrow x = y;\ x * a = y * a \Rightarrow x = y)$ erfüllt, ist. Eine Quasigruppe $(P, *)$ heißt idempotent, wenn $a * a = a$ für alle $a \in P$. Zwei Quasigruppen $(P, *)$ und $(P, \circ)$ heißen orthogonal, wenn für alle $a, b \in P$ das Gleichungssystem $x * y = a$, $x \circ y = b$ eine eindeutige Lösung (x, y) hat. Eine Quasigruppe heißt kommutativ, wenn $a * b = b * a$ für alle $a, b \in P$.

3.3.6. *Äquivalenzsatz.* v, k seien natürliche Zahlen, $v \geqslant 2$, $k \geqslant 3$.

Die folgenden kombinatorischen Strukturen sind äquivalent:

(i) ein (primäres) $(v, k, 1)$-HTS,

(ii) ein $(k, 1; v)$-TD,

(iii) ein $(k, 1, v; kv)$-GDD,

(iv) ein $(v, k, 1)$-Netz,

(v) eine $(v^2, k, v, 2)$-OA vom Index 1,

(vi) eine Menge von $k - 2$ paarweise orthogonalen Lateinischen Quadraten der Ordnung,

(vii) eine Menge von $k - 2$ paarweise orthogonalen Quasigruppen auf einer v-Menge.

Beweis. Die Äquivalenz (i) $\Leftrightarrow$ (ii) wurde in 3.1.8 gezeigt. (ii) $\Leftrightarrow$ (iii)

ist die Aussage von 3.1.4, 3.2.8.(a) ergibt (i) $\Leftrightarrow$ (iv), und 3.3.3 liefert (i) $\Leftrightarrow$ (v). Wir zeigen nun (vi) $\Rightarrow$ (vii) $\Rightarrow$ (i) $\Rightarrow$ (vi).

(vi) $\Rightarrow$ (vii): Für jedes Lateinische Quadrat $A = (a_{ij})$ über $P = \{p_1, \ldots, p_v\}$ sei auf $V = \{1, \ldots, v\}$ die Operation $*_A$ erklärt durch $i *_A j = n \Leftrightarrow a_{ij} = p_n$. Die Eigenschaft (L1) für Zeilen (Spalten) liefert dann die eindeutige Lösbarkeit von $y *_A a = b$ ($a *_A x = b$). Das ist zu den Kürzungsregeln äquivalent. Daher ist $(V, *_A)$ Quasigruppe.—Sind A und B orthogonale Lateinische Quadrate, so hat $x *_A y = m$, $x *_B y = n$ die Lösung $(x, y) = (i, j)$ genau dann, wenn $(a_{ij}, b_{ij}) = (p_m, p_n)$; (x, y) ist daher eindeutig bestimmt. Also sind die Quasigruppen $(V, *_A)$ und $(V, *_B)$ orthogonal.

(vii) $\Rightarrow$ (i): $(P, *_i)$, $i = 1, \ldots, k-2$, seien paarweis orthogonale Quasigruppen auf der v-Menge P. Eine triviale Rechnung zeigt dann, daß für das Tupelsystem

$$Q = \{(a_1 * b, \ldots, a_{k-2} * b, a, b) \mid a, b \in P\}$$

$\mu_{ij}(a, b) = 1$ für alle $a, b \in P$, $i, j = 1, \ldots, k$, $i \neq j$ gilt (Fallunterscheidung für $i, j \leqslant k-2$; $i \leqslant k-2$, $j = k-1$; $i \leqslant k-2$, $j = k$; $i = k-1$, $j = k$). Daher ist Q ein $(v, k, 1)$-HTS.

(i) $\Rightarrow$ (vi): Q sei $(v, k, 1)$-HTS über $P = \{a_1, \ldots, a_v\}$. Definiere für $n = 1, \ldots, k-2$ Lateinische Quadrate $A^{(n)} = (a_{ij}^{(n)})$ durch

$$a_{ij}^{(n)} = x_n, \text{ wenn } x \in Q,\ x_{k-1} = a_i,\ x_k = a_j. \tag{2}$$

(2) bestimmt x eindeutig, daher sind die $A^{(n)}$ wohldefiniert. Aus $\mu_{n,k-1}(a, b) = \mu_{nk}(a, b) = 1$ $(n \leqslant k-2)$ ergibt sich, daß $A^{(n)}$ Lateinisches Quadrat ist, und $\mu_{ij}(a, b) = 1$ für $1 \leqslant i < j \leqslant k-2$ liefert die Orthogonalität von $A^{(i)}$ und $A^{(j)}$ für $i \neq j$.

Ohne Mühe kann man noch die folgenden Charakterisierungen spezieller Eigenschaften von Quasigruppen und Lateinischen Quadraten nachprüfen:

3.3.7. *Satz* (a) Das durch (1) definierte $(v, k, 1)$-HTS ist genau dann idempotent, wenn alle Operationen $*_i$ idempotent sind.

(b) Das zu einer Quasigruppe $(P, *)$ gehörige $(v, 3, 1)$-HTS besitzt genau dann den freien Automorphismus (23), wenn $*$ kommutativ ist.

(c) Ist Q ein $(v, 4, 1)$-HTS, so sind die durch (2) definierten Lateinischen Quadrate $A^{(1)}$ und $A^{(2)}$ genau dann zueinander transponiert, wenn Q den freien Automorphismus (12) (34) hat. D.h., selbstorthogonale Lateinische Quadrate der Ordnung v sind äquivalent zu $(v, 4, 1; \langle(12)(34)\rangle)$-HTS.

3.4. Blockpläne und SBTS

3.4.1. *Satz.* Existiert ein $(v, k, \mu; G)$-SBTS, so existiert auch ein

$(v, k, \frac{\mu k(k-1)}{|G|})$-Blockplan.

Beweis. Q sei $(v, k, \mu; G)$-SBTS. Jeder Bahn Gx von G in Q ordnen wir die k-Menge $B(Gx) = \{x_1, \ldots, x_k\}$ zu. Offensichtlich ist $B(Gx)$ unabhängig von der Wahl von x aus der Bahn. Das Paar $(P, \{B(Gx) \mid$ alle Bahnen $Gx\})$, wo mehrfache Bahnen mehrfach gezählt werden, ist dann ein $(v, k, \frac{\mu k(k-1)}{|G|})$-Blockplan. Denn P enthält v Punkte, und jeder Block enthält k Punkte. Sind nun a, b zwei verschiedene Punkte von P, so ist genau dann $a, b \in B(Gx)$, wenn $i, j \in I$, $i \neq j$ existieren mit $x_i = a$, $x_j = b$. Für festes $i \neq j$ gibt es genau μ Lösungen, insgesamt also $\mu k(k-1)$. Aber davon liegen je $|G|$ in derselben Bahn. Daher ist die Zahl der a und b enthaltenden Blöcke $\lambda = \frac{\mu k(k-1)}{|G|}$.

3.4.2. *Äquivalenzsatz für Blockpläne.* G sei 2-fach transitive Untergruppe der symmetrischen Gruppe S_k. Dann existiert ein (v, k, λ)-Blockplan genau dann, wenn ein $(v, k, \lambda \frac{|G|}{k(k-1)}; G)$-SBTS existiert.

Beweis. $(P, \mathcal{B})$ sei ein (v, k, λ)-Blockplan. Numeriere jeden Block $B \in \mathcal{B}$ in irgendeiner Weise als $B = \{a_{B,1}, \ldots, a_{B,k}\}$. Dann ist das Tupelsystem $Q = \{(a_{B,\alpha 1}, \ldots, a_{B,\alpha k}) \mid B \in \mathcal{B}, \alpha \in G\}$ ein $(v, k, \lambda \frac{|G|}{k(k-1)}; G)$-SBTS über P. Denn offensichtlich ist G eine Gruppe freier Automorphismen von Q. Die Zahl der $x \in Q$ mit $x_i = a$, $x_j = b$ $(i \neq j)$ ist gleich der Zahl der $(B, \alpha) \in \mathcal{B} \times G$ mit $a_{B,\alpha i} = a$, $a_{B,\alpha j} = b$. Nun gibt es für $a \neq b$ genau λ Blöcke $B \in \mathcal{B}$ mit $a, b \in B$, etwa $a = a_{B,i_0}$, $b = a_{B,j_0}$ $(i_0 \neq j_0)$. Weiter gibt es für festes B genau $\frac{|G|}{k(k-1)}$ Permutationen $\alpha \in G$ mit $\alpha i = i_0$, $\alpha j = j_0$. Daher ist $\mu_{ij}(a, b) = \lambda \cdot \frac{|G|}{k(k-1)}$. Die Umkehrung folgt aus Satz 3.4.1.

Wir heben zwei Spezialfälle hervor:

3.4.3. *Folgerung.* (a) Ein $(v, k, \lambda(k-2)!; S_k)$-SBTS existiert genau dann, wenn ein (v, k, λ)-Blockplan existiert.

(b) q sei Primzahlpotenz, und $A(q)$ sei die Gruppe der ganzlinearen Substitutionen $x \to ax + b$ $(a, b \in GF(q), a \neq 0)$ des endlichen Körpers $GF(q)$.—Ein $(v, q, 1; A(q))$-SBTS existiert genau dann, wenn ein $(v, q, 1)$-Blockplan existiert.

Wir benützen nun Satz 3.4.1., um aus den Nichtexistenzsätzen für Blockpläne weitere notwendige Kriterien für die Existenz von SBTS zu erhalten.

3.4.4. *Satz.* Es sei $k \geqslant 2$, $\mu \geqslant 1$.

Existiert ein $(v, k, \mu; G)$-SBTS, so ist entweder

$$v \in \{1, k\} \tag{1}$$

oder

$$v \geqslant \text{Max}\,(k+1, \frac{|G|}{\mu} + 1). \tag{2}$$

Ist $v = \frac{|G|}{\mu} + 1$ und setzt man

$$n = \frac{k(v-k)}{v-1}, \tag{3}$$

so gilt:

(i) Ist v gerade, so ist n ein Quadrat,

(ii) Ist v ungerade, so hat die diophantische Gleichung

$$nx^2 + (-1)^{\frac{v-1}{2}} vy^2 = z^2 \tag{4}$$

eine nichttriviale ganzzahlige Lösung.

Beweis. Ist $v > 1$, so gibt es ein Tupel $x \in Q$ mit $x_1 = a$, $x_2 = b$, wo a, b beliebige verschiedene Punkte sind. Wegen (SBTS2) sind die $x_i (i \in I)$ alle verschieden, und daher ist $v \geqslant k$. Es sei nun $v \geqslant k+1$. Nach Satz 3.4.1. existiert ein $(v, k, \frac{\mu k(k-1)}{|G|})$-Blockplan mit $b = \frac{v(v-1)}{k(k-1)} = \frac{\mu v(v-1)}{|G|}$ Blöcken. Nach der Fisher-Ungleichung (2.3.7. (a)) ist dann $b \geqslant v$, woraus sich $v \geqslant \frac{|G|}{\mu} + 1$ ergibt. Daher gilt (2).

Ist $v = \frac{|G|}{\mu} + 1$, so ist $b = v$, und aus der Bruck-Ryser-Bedingung (2.3.7. (b)) ergibt sich (i), (ii) mit $n = r - \lambda$. Aus $\lambda = \frac{\mu k(k-1)}{|G|} = \frac{k(k-1)}{v-1}$ und $r = \frac{\lambda(v-1)}{k-1} = k$ berechnet sich dann n zu (3).

Nach 3.4.1. müssen die Parameter des zu einem $(v, k, \mu; G)$-SBTS gehörigen (v, k, λ)-Blockplans die Bedingung $\lambda|G| = \mu k(k-1)$, oder

$$|G| \equiv 0 \bmod \frac{k(k-1)}{(k(k-1), \lambda)} \tag{5}$$

erfüllen. Deshalb sagen wir, ein (v, k, λ)-Blockplan sei *minimal darstellbar*, wenn er nach 3.4.1. aus einem $(v, k, \lambda; G)$-SBTS mit einer Gruppe G der Ordnung

$$|G| = \frac{k(k-1)}{(k(k-1), \lambda)} \tag{6}$$

entsteht (es ist dann $\mu = \frac{\lambda}{(\lambda, k(k-1))}$).

3.4.5. *Satz.* Ein $(v, k, 1)$-Blockplan ist genau dann minimal darstellbar, wenn k eine Primzahlpotenz ist.

Beweis. Aus (6) ergibt sich $|G| = k(k-1)$, und wegen $\lambda|G| = \mu k(k-1)$ ist dann $\mu = 1$. Nach Proposition 2.2.2. ist daher $|G_{ij}| = 1$ für alle $i \neq j$. Da G Permutationsgruppe vom Grad k ist, muß G scharf zweifach transitiv sein, und nach einem bekannten Satz ist dann k eine Primzahlpotenz. Aus 3.4.3. (b) ergibt sich umgekehrt, daß ein $(v, k, 1)$-Blockplan minimal darstellbar ist, wenn k eine Primzahlpotenz ist.

Man kann fragen, ob jeder Blockplan, bei dem k Primzahlpotenz ist, minimal darstellbar ist. Das ist nicht der Fall: Eine minimale Darstellung des (existierenden!) (6, 3, 2)-Blockplans müßte ein (6, 3, 1; Z_3)-SBTS sein, was nicht existiert (s. Kapitel 6).

Wir beweisen in Kapitel 4 (Satz 4.1.4.) die Existenz eines $(q, \frac{q-1}{2}, 1; D_{\frac{q-1}{2}})$-SBTS für Primzahlpotenzen $q \equiv 3 \bmod 4$. Nach Satz 3.4.1. gehören dazu minimal darstellbare $(q, \frac{q-1}{2}, \frac{q-3}{4})$-(Hadamard)-Blockpläne. Ein interessantes Problem ist die Frage, ob für jede natürliche Zahl n ein mit der Diedergruppe D_{2n-1} darstellbarer $(4n-1, 2n-1, 2n)$-Hadamard-Blockplan existiert. Das hätte die Existenz eines $(4n-1, 2n-1, 1; D_{2n-1})$-SBTS für jedes n zur Folge, und nach 3.3.6. insbesondere die Existenz von $2n-3$ paarweise orthogonalen Lateinischen Quadraten der Ordnung $4n-1$ (eine Zahl, die bisher nur für Primzahlpotenzen $4n-1$ erreicht ist) !

3.5. Roomsche Quadrate

3.5.1. *Definition (Roomsches Quadrat).* P_0 sei eine $(v+1)$-Menge.

Ein Roomsches Quadrat (über P_0) der Seite v ist eine $v \times v$-Matrix R, deren Zellen entweder leer sind, oder ein ungeordnetes Paar von Elementen von P_0 enthalten, derart daß

(RS1) Jedes $a \in P_0$ kommt in jeder Zeile, und in jeder Spalte von R genau einmal vor,

(RS2) Jedes ungeordnete Paar von Elementen von P_0 tritt genau einmal in R auf.

R heißt standardisiert bezüglich $\infty \in P_0$, wenn die Diagonale von R gerade die Paare $\{a, \infty\}$, $a \in P_0 - \{\infty\}$ enthält.

Aus der Definition ergibt sich sofort, daß P_0 eine gerade Anzahl von Elementen enthält. Also gilt :

3.5.2. Die Seitenlänge v eines Roomschen Quadrats ist ungerade.

Zur Theorie der Roomschen Quadrate siehe Wallis [25]. Von dort übernehme ich auch:

3.5.3. *Standardisierung.* R sei Roomsches Quadrat über P_0, und $\infty \in P_0$ ein beliebiges Element. Dann läßt sich R durch Permutationen der Zeilen und Spalten in ein bezüglich ∞ standardisiertes Roomsches Quadrat umformen.

3.5.4. *Äquivalenzsatz für Roomsche Quadrate.* Ein Roomsches Quadrat der Seite v existiert genau dann, wenn ein $(v, 4, 1, M_1; \langle(12)\rangle)$-SBTS existiert mit

$$M_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}. \tag{1}$$

Beweis. (a) Q sei ein $(v, 4, 1, M_1; \langle(12)\rangle)$-SBTS über $P = \{a_1, \ldots, a_v\}$. Wir füllen die Zellen einer $v \times v$-Matrix R auf folgende Weise: Zelle (i, i) von R enthält $\{a_i, \infty\}$, Zelle (i, j) von R enthält $\{a, b\} \Leftrightarrow (a, b, a_i, a_j) \in Q$ $(i \neq j)$, und die übrigen Zellen bleiben leer. Daß (12) ein freier Automorphismus ist, besagt zusammen mit $\mu_{34} = 2$ gerade, daß jede Zelle (i, j) höchstens ein ungeordnetes Paar enthält. $\mu_{13} = \mu_{14} = 1$ ergeben (RS1), und (RS2) folgt aus $\mu_{12} = 1$. Daher ist R ein (standardisiertes) Roomsches Quadrat.

(b) Wegen 3.5.3. können wir o.B.d.A. annehmen, daß R ein bez. ∞ standardisiertes Roomsches Quadrat ist. Setze $P = P_0 - \{\infty\}$. Angenommen, in Zelle (i, i) liegt $\{a_i, \infty\}$ $(i = 1, \ldots, v)$. Dann ist $P = \{a_1, \ldots, a_v\}$. Wir setzen nun $Q = \{(a, b, a_i, a_j) \mid \{a, b\} \text{ liegt in } (i, j)\}$. Wegen $\{a, b\} = \{b, a\}$ hat Q den freien Automorphismus (12). Die Einträge im Tupel (a, b, a_i, a_j) sind alle verschieden (und daher gilt (SBTS2)); denn $a \neq b$ und $a_i \neq a_j$ sind klar, und wäre $a_i = a$, so enthielte die i-te Zeile die Paare $\{a, b\}$ und $\{a, \infty\}$, im Widerspruch zu (RS1). Daher ist $a_i \neq a$, und die übrigen Ungleichungen folgen ebenso.

Aus (RS2) ergibt sich nun $\mu_{12}(a, b) = 1$ für $a \neq b$, und aus (RS1) folgt $\mu_{12} = \mu_{14} = \mu_{23} = \mu_{24} = 1$. Schließlich ist $\mu_{34}(a_i, a_j) = 0$, wenn Zelle (i, j) leer ist, und $= 2$, wenn sie $\{a, b\} = \{b, a\}$ enthält. Daher ist Q ein $(v, 4, 1, M_1; \langle(12)\rangle)$-SBTS.

4. KONSTRUKTIONSMETHODEN FÜR SBTS UND HTS

Direkte Konstruktionen für SBTS und HTS mittels endlicher abelscher Gruppen und Körpern werden in Abschnitt 4.1. behandelt. Wir haben uns auf einige exemplarische Serien beschränkt (siehe Anhang).

In Abschnitt 4.2. werden Differenzenverfahren für SBTS eingeführt. Das erste Verfahren (mit gewöhnlichen Startern) liefert ein Tupelsystem mit transitiver reiner Automorphismengruppe; das zweite (mit unvollständigen Startern) liefert ein Tupelsystem, das durch ein vorgegebenes (kleines) SBTS zu einem großen SBTS ergänzt werden kann. Die Konstruktionen werden durch Beispiele erläutert. Auf Starterkonstruktionen für HTS wurde verzichtet.

Abschnitt 4.3. bringt rekursive Konstruktionen. Wir präsentieren hier nur wenige dieser Konstruktionen, da eine systematische Darstellung die Einführung neuer Begriffe erfordert (siehe Anhang). Behandelt werden die PBD-Konstruktion, die GDD-Konstruktion sowie eine Konstruktion für HTS, die auch maximale HTS liefert. Als Konsequenz ergibt sich eine rekursive Konstruktion für affine Blockpläne.

4.1. Direkte Konstruktionen

4.1.1. *Lemma.* K sei endlicher (kommutativer und assoziativer) Ring mit Einselement, und R sei ein endlicher K-modul mit v Elementen. Erfüllt dann die Teilmenge I von K die Bedingung

$$i - j \in K^\times \text{ für alle } i, j \in I,\ i \neq j, \tag{1}$$

so ist mit $k = |I|$

$$Q = \{(ia + b : i \in I) \mid a, b \in R,\ a \neq 0\} \tag{2}$$

ein $(v, k, 1)$-SBTS über R, und

$$Q' = \{(a, ia + b : i \in I) \mid a, b \in R\} \tag{2a}$$

ist ein $(v, k + 1, 1)$-HTS.

Beweis. Ist $i - j \in K^\times$, so hat $ix + y = a$, $jx + y = b$ die eindeutige Lösung $x = (i - j)^{-1}(a - b)$, $y = a - ix$, und x ist genau dann von 0 verschieden, wenn $a \neq b$. Daher ist $\mu_{ij}(a, b) = \delta(a, b)$, wo δ das Kroneckersymbol ist, und Q ist SBTS. Ebenso sieht man, daß Q' ein HTS ist.

4.1.2. *Beispiel.* v sei ungerade, und K sei der Ring der ganzen Zahlen modulo v. Ist p der kleinste Primteiler von v, so erfüllt $I = \{0, 1, \ldots, p - 1\}$ die Bedingung (1). Daher ist (2a) für jede abelsche Gruppe R der Ordnung v ein $(v, p + 1, 1)$-HTS.

Ist K ein endlicher Körper, so ist (1) für jede Teilmenge I von K erfüllt. Wir geben nun spezielle Teilmengen I so an, daß das SBTS (2) freie Automorphismen besitzt.

4.1.3. *Satz.* q sei Primzahlpotenz. Für alle natürlichen Zahlen d, k mit

$$d | q - 1,\ d | k \leqslant q - 1 \tag{3}$$

existiert dann ein $(q, k, 1; Z_k(d))$-SBTS, wo $Z_k(d)$ eine semireguläre zyklische Gruppe der Ordnung d vom Grad k ist.

Beweis. Es sei $K = GF(q)$ der endliche Körper mit q Elementen. Wegen $d \mid q-1$ enthält $K^\times$ eine zyklische Gruppe H der Ordnung d. I sei die Vereinigung von $d^{-1}k$ Restklassen von $K^\times/H$. Dann ist $|I| = k$, und mit $R = K$ wird durch (2) ein $(q, k, 1)$-SBTS definiert. Die Substitution $i \to \alpha i$ ($\alpha \in H$) ist eine Permutation von I und führt offensichtlich jedes Tupel aus Q wieder in ein solches über. Daher ist die Menge der Substitutionen $i \to \alpha i$ eine Gruppe freier Automorphismen von Q, die offensichtlich isomorph zu $Z_k(d)$ ist.

Bemerkung. Nimmt man zu der eben konstruierten Stellenmenge I noch die 0 dazu, so erhält man ein $(q, k+1, 1)$-SBTS, und die Substitutionen $i \to \alpha i$ ($\alpha \in H$) sind immer noch freie Automorphismen.

4.1.4. *Satz.* q sei ungerade Primzahlpotenz. Für alle ungeraden Teiler k von $q-1$ existiert dann ein $(q, k, 1; D_k)$-SBTS, wo D_k die Diedergruppe vom Grad k ist.

Beweis. Es sei wieder $K = GF(q)$, und α sei eine primitive k-te Einheitswurzel von K. Weil k ungerade und $q-1$ gerade ist, sind die Elemente $\pm 1, \pm\alpha, \ldots, \pm\alpha^{k-1}$ verschieden und bilden eine Untergruppe H von K. Wir wählen nun ein Repräsentantensystem S_0 von $K^\times/H$ und setzen $S = S_0 \cup \alpha S_0 \cup \ldots \cup \alpha^{k-1} S_0$. S hat die Eigenschaften

$$\alpha S = S,\ S \cap -S = \emptyset,\ S \cup -S = K - \{0\}. \tag{4}$$

Setze nun

$$Q = \{(\alpha^{\epsilon i} x + y : i \bmod k) \mid x \in S,\ y \in K,\ \epsilon = \pm 1\}.$$

Offensichtlich enthält jedes Tupel von Q lauter verschiedene Elemente. Daher gilt (SBTS2). Wir zeigen nun $\mu_{ij}(a, b) = 1$ für $i \neq j$, $a \neq b$. $\mu_{ij}(a, b)$ ist die Anzahl der Lösungen $(x, y, \epsilon) \in S \times K \times \{\pm 1\}$ von

$$\alpha^{\epsilon i} x + y = a,\ \alpha^{\epsilon j} x + y = b. \tag{5}$$

Aus (5) ergibt sich

$$x = (\alpha^{\epsilon t} - \alpha^{\epsilon j})^{-1}(a - b). \tag{6}$$

Nun ist $\alpha^{-i} - \alpha^{-j} = -\alpha^{-i-j}(\alpha^i - \alpha^j)$, also liegt wegen (4) genau einer der Ausdrücke (6; $\epsilon = 1$) und (6; $\epsilon = -1$) in S. Daher sind ϵ und x durch (5) eindeutig bestimmt, und aus (5) ergibt sich auch y eindeutig. Daher ist $\mu_{ij}(a, b) = 1$, und Q ist SBTS. Schließlich ergibt sich ohne weiteres, daß die Substitutionen $i \to \alpha i$, $i \to i^{-1}$ freie Automorphismen von Q sind, die D_k erzeugen.

Wir konstruieren nun noch eine Klasse maximaler HTS:

4.1.5. *Satz.* q sei Primzahlpotenz. Dann existiert für jede natürliche Zahl $s \geqslant 2$ ein maximales $\left(q, \frac{q^s - 1}{q - 1}, q^{s-2}\right)$-*HTS*.

Beweis. Es sei $k = GF(q)$, und $K = GF(q^s)$ sei die Erweiterung von k

vom Grad s. Die Spur $s(x) = x + x^q + \ldots + x^{q^{s-1}}$ ist ein k-linearer Homomorphismus von K auf k. I sei ein Repräsentantensystem von $K^\times/k^\times$. Es ist $|I| = (K^\times : k^\times) = \dfrac{q^s - 1}{q - 1}$. Das Tupelsystem

$$Q = \{(s(ix) : i \in I) \mid x \in K\} \tag{7}$$

ist ein $\left(q, \dfrac{q^s - 1}{q - 1}, q^{s-2}\right)$-*HTS*. Dazu genügt es zu zeigen, daß das lineare Gleichungssystem

$$s(ix) = a,\ s(jx) = b \tag{8}$$

für $i \neq j$ den Rang 2 hat. Dann ist nämlich die Lösungsmenge von (8) eine Nebenklasse eines $(s-2)$-dimensionalen k-Untervektorraum von K, und daher $\mu_{ij}(a, b) = q^{s-2}$.

Angenommen, (8) hat einen Rang < 2. Dann gibt es $c, d \in k$, nicht beide gleich Null, so daß für alle $x \in K$ gilt:

$$0 = c \cdot s(ix) + d \cdot s(jx) = s((ci + dj)x).$$

Aberweil die Spur surjektiv ist, ergibt sich für $ci + dj \neq 0$ ein Widerspruch. Daher ist

$$ci + dj = 0. \tag{9}$$

Wegen $i, j \in I \not\ni 0$ ist dann $c, d \neq 0$. (9) besagt daher, daß i und j in derselben Nebenklasse von $K^\times/k^\times$ liegen. Nach Wahl von I ist daher $i = j$. Also hat (8) für $i \neq j$ den Rang 2.

4.1.6. *Zusatz.* Unter den Voraussetzungen von 4.1.5. sei d eine natürliche Zahl mit

$$d \mid \frac{q^s - 1}{q - 1},\ (d, q - 1) = 1. \tag{10}$$

Dann kann man I so wählen, daß das HTS (7) eine freie Automorphismengruppe isomorph zu $Z_k(d)$ hat.

Beweis. H_0 sei die Gruppe der $d(q-1)$-ten Einheitswurzeln von K, und H sei die Untergruppe der Ordnung d. Weil jedes Element von $k^\times$ eine $(q-1)$-te Einheitswurzel ist, ist $k^\times$ Untergruppe von H_0; und wegen $(d, q-1) = 1$ ist $H_0 = H \times k^\times$.

Die Nebenklassen von H_0 in K seien $\alpha_1 H_0, \ldots, \alpha_r H_0 \left(r = \dfrac{q^s - 1}{(q-1)\,d}\right)$. Definiere I als die Vereinigung von $\alpha_1 H, \ldots, \alpha_r H$. Nach Konstruktion erfüllt I die Bedingung

$$i \in I,\ \alpha \in H \Rightarrow \alpha i \in I. \tag{11}$$

Wegen $H_0 = H \times k^\times$ enthält i aus jeder Nebenklasse von $k^\times$ genau ein Element. Daher ist das Tupelsystem Q von (7) ein HTS. Und aus (11) ergibt sich leicht, daß die Substitution $i \to \alpha i$ $(\alpha \in H)$ ein freier Automor-

phismus des HTS (7) ist, der $Z_k(d)$ erzeugt.

4.1.7. *Folgerung.* Ein (q^{s-2}, q)-ARBIBD existiert für jede Primzahlpotenz q und jede natürliche Zahl $s \geqslant 2$.

Beweis. Das ergibt sich sofort aus Satz 4.1.5. zusammen mit Satz 3.2.8. (c).

4.2. Starterkonstruktionen

K sei endliche abelsche Gruppe der Ordnung $q = ef + 1$, und A sei eine Gruppe der Ordnung f, bestehend aus fixpunktfreien Automorphismen von K. G sei eine auf der k-Menge I treue Permutationsgruppe.

4.2.1. *Definition (Starter).* Ein $K \times A$-Starter für ein $(q, k, \mu, M; G)$-SBTS ist ein (q, k)-Tupelsystem (K, I, Q^*, ϵ) mit den Eigenschaften

(S_0) Jedes $x \in Q^*$ hat lauter verschiedene Einträge,

(S_1) $|Q^*| = |G|^{-1}\mu e$,

(S_2) Sind i und j verschiedene Stellen von I, so ist für alle $a \in K - \{0\}$ die Zahl der $(x, \alpha) \in Q^* \times G$ mit

$$A(x_{\alpha i} - x_{\alpha j}) = Aa \tag{1}$$

enthalten in $\{0, \mu_{ij}\}$.

Ist A trivial, so nennen wir (K, I, Q^*, ϵ) einen K-Starter.

4.2.2. *Satz.* Ist Q^* ein $K \times A$-Starter für ein $(q, k, \mu, M; G)$-SBTS, so ist

$$Q = \{(tx_{\alpha i} + c : i \in I) \mid x \in Q^*, t \in A, c \in K, \alpha \in G\} \tag{2}$$

ein $(q, k, \mu, M; G)$-SBTS.

Beweis. Aus (2) ergibt sich sofort (SBTS1), und (SBTS2) ist eine Folge von (S_0).

Die Zahl $\rho_i(a)$ der $z \in Q$ mit $z_i = a$ ist gleich der Zahl der Lösungen (x, t, c, α) von $tx_{\alpha i} + c = a$. Das hat für jedes x, t, α genau eine Lösung c. Daher ist $\rho_i(a) = |A| \cdot |G| \cdot |Q^*| = \mu(q - 1)$.

Die Zahl $\mu_{ij}(a, b)$ der $z \in Q$ mit $z_i = a$, $z_j = b$ ist gleich der Zahl der Lösungen (x, t, c, α) von $tx_{\alpha i} + c = a$, $tx_{\alpha j} + c = b$. Eine dieser Gleichungen bestimmt c; daher ist $\mu_{ij}(a, b)$ gleich der Zahl der Lösungen (x, t, α) von $t(x_{\alpha i} - x_{\alpha j}) = a - b$, also $\in \{0, \mu_{ij}\}$ für $a \neq b$. Daher gilt auch (SBTS3).

Bemerkungen. (a) Die Substitutionen $x \to tx + a$ $(a \in K, t \in A)$ bilden eine zum semidirekten Produkt $K \times A$ isomorphe Gruppe reiner Automorphismen !

(b) Die Tupelsysteme $T_{x,t,\alpha} = \{(tx_{\alpha i} + c : i \in I) \mid c \in K\}$ $(x \in Q, t \in A, \alpha \in G)$ bilden eine disjunkte Zerlegung von Q in Transversalen.

4.2.3. *Beispiel.* K sei die Gruppe $Z_2 \times Z_6$ (direktes Produkt). Die folgenden Tupel bilden einen K-Starter für ein (12, 6, 1)-SBTS:

(00, 01, 10, 03, 12, 04), (00, 10, 13, 02, 03, 12),
(00, 02, 12, 10, 01, 15), (00, 11, 15, 12, 14, 10),
(00, 03, 02, 01, 15, 14), (00, 12, 04, 05, 02, 13),
(00, 04, 11, 13, 05, 02), (00, 13, 14, 04, 11, 01),
(00, 05, 01, 15, 13, 11), (00, 14, 05, 11, 10, 03),
(00, 15, 03, 14, 04, 05).

(s. Hanani [11], Lemma 3.21)

4.2.4. *Beispiel.* q sei eine ungerade Primzahlpotenz, die nicht von der Form $2^s + 1$ ist, und t sei der größte ungerade Teiler von $q - 1$. α sei eine primitive t-te Einheitswurzel in $K = GF(q)$. Wie im Beweis von Satz 4.1.4. zeigt man die Existenz einer Teilmenge S von K mit

$$\alpha S = S,\ S \cap -S = \emptyset,\ S \cup -S = K - \{0\}. \tag{3}$$

Dann ist $Q^* = \{(0, (\alpha + 1)z, \alpha z, z) \mid z \in S\}$ ein K-Starter für ein $(q, 4, 1, M_1; \langle(12)\rangle)$-SBTS, we M_1 die Matrix (1) aus Satz 3.5.4. ist.

Beweis. Wegen $q \neq 2^s + 1$ ist $t > 1$, und daher $\alpha \neq 1$. Da t ungerade, und $q - 1$ gerade ist, ist $\alpha \neq -1$. (S0) und (S1) sind offenbar erfüllt. (S2) beweist man durch Fallunterscheidung. Wir beweisen z.B. den Fall $i = 1, j = 4$.

Ist $x = (0, (\alpha + 1)z, \alpha z, z)$, $z \in S$, so ist $x_1 - x_4 = -z$, $x_2 - x_4 = \alpha z$; daher ist (1) äquivalent dazu, daß die Zahl der Lösungen $z \in S$ von $a \in \{\alpha z, -z\}$ in $\{0, \mu_{14}\} = \{0, 1\}$ liegt. Aber das folgt sofort aus (3).

Es seien nun $\infty^{(1)}, \ldots, \infty^{(r)}$ verschiedene, nicht in K liegende Elemente. Wir setzen $P^* = K \cup \{\infty^{(1)}, \ldots, \infty^{(r)}\}$. Ist dann (P^*, I, Q^*, ϵ) ein Tupelsystem mit der Eigenschaft

$$\mu_{ij}(\infty^{(\nu)}, \infty^{(\nu')}) = 0 \text{ für alle } i \neq j, \nu \neq \nu', \tag{4}$$

so setzen wir

$$Q^{(0)} = \{x \in Q^* \mid x_i \in P \text{ für alle } i\},$$
$$Q_i^{(\nu)} = \{x \in Q^* \mid x_i = \infty^{(\nu)}\},$$

so daß Q^* die disjunkte Vereinigung aller dieser Elemente ist.

4.2.5. *Definition (unvollständiger Starter).* Ein unvollständiger $K \times A$-Starter für ein $(q + rf, k, \mu; G)$-SBTS ist ein Tupelsystem (P^*, I, Q^*, ϵ) mit (4) und

(S0′) Jedes $x \in Q^*$ hat lauter verschiedene Einträge,

(S1′)

$$|Q^{(0)}| = |G|^{-1}\mu(e - r(k - 2)) \tag{5}$$

$$\sum_{j \in Gi} |Q_j^{(\nu)}| = |G_i|^{-1}\mu, \ (i \in I, \nu = 1, \ldots, r) \tag{6}$$

(S2′) Sind i und j verschiedene Stellen von I, und ist $a \in K - \{0\}$, so gibt es genau μ Paare $(x, \alpha) \in Q^* \times G$ mit

$$x_{\alpha i}, x_{\alpha j} \in K, \ A(x_{\alpha i} - x_{\alpha j}) = Aa. \tag{7}$$

4.2.6. *Satz.* $P_0 = \{\infty_t^{(\nu)} \mid t \in A, \nu = 1, \ldots, r\}$ sei eine Menge verschiedener, nicht in K liegender Elemente. (P_0, I, Q_0, ϵ) sei ein $(rf, k, \mu; G)$-SBTS, und Q^* sei ein unvollständiger $K \times A$-Starter für ein $(q + rf, k, \mu; G)$-SBTS. Dann existiert ein $(q + rf, k, \mu; G)$-SBTS.

Beweis. Wir setzen für $t \in A, c \in K$:

$$t\infty^{(\nu)} + c = \infty_t^{(\nu)}, \tag{8}$$

und definieren

$$Q = Q_0 \cup \{(tx_{\alpha i} + c : i \in I) \mid x \in Q'^*, t \in A, c \in K, \alpha \in G\}. \tag{9}$$

Aus (9) ergeben sich unmittelbar (SBTS1) und (SBTS2). Wir zeigen nun $\mu_{lj}(a, b) = \mu$ für $l \neq j$, $a \neq b$.

Fall 1: $a \in K$, $b = \infty_t^{(\nu)}$. Das Tupel $z \in Q$ erfüllt genau dann $z_l = a$, $z_j = b$, wenn $z = (tx_{\alpha i} + a - tx_{\alpha l} : i \in I)$, wo $x \in Q_j^{(\nu)}$, $\alpha \in G$. Daher ist $\mu_{lj}(a, b) = \sum_{\alpha \in G} Q_{\alpha j}^{(\nu)} = |G_j| \cdot \sum_{i \in Gj} |Q_i^{(\nu)}| = \mu$ nach (6).

Fall 2: $a = \infty_t^{(\nu)}$, $b \in K$. Nach Fall 1 ist $\mu_{lj}(a, b) = \mu_{jl}(b, a) = \mu$.

Fall 3: $a, b \in P_0$. Das Tupel $z \in Q$ erfüllt genau dann $z_l = a$, $z_j = b$, wenn $z \in Q_0$. Daher ist $\mu_{lj}(a, b) = \mu(Q_0) = \mu$.

Fall 4: $a, b \in K$. Die Anzahl $\mu_{lj}(a, b)$ der $z \in Q$ mit $z_l = a$, $z_j = b$ ist gleich der Zahl der Lösungen von $tx_{\alpha l} + c = a$, $tx_{\alpha j} + c = b$. Eine dieser Gleichungen bestimmt eindeutig c; daher ist $\mu_{lj}(a, b)$ gleich der Zahl der Lösungen von $t(x_{\alpha l} - x_{\alpha j}) = a - b$, nach (S2′) also gleich μ.

Damit ist Q als $(q, k, \mu; G)$-SBTS nachgewiesen.

Bemerkung. Für $r = 0$ ergibt sich wieder der Spezialfall $M = (\mu)$ von Satz 4.2.2.

4.2.7. *Beispiel.* $Q^* = \{(\infty^{(a)}, a, -a, 0) \mid a = 1, \ldots, m\}$ ist ein unvollständiger Z_{2m+1}-Starter für ein $((2m + 1) + m, 4, 1; V_4)$-SBTS mit der Kleinschen Vierergruppe V_4.

Beweis. Man rechnet leicht (S1′) nach $(e = 2m, r = m, k = 4, \mu = 1, |G| = 4, |G_i| = 1)$. (So′) gilt offensichtlich. Ist nun $I = \{0, 1, 2, 3\}$, so ist $G = V_4 = \{E, (01)(23), (02)(13), (03)(12)\}$. G induziert auf den Paaren verschiedener Stellen die Bahnen $\{01, 10, 23, 32\}$, $\{02, 20, 13, 31\}$ und $\{03, 30, 12, 21\}$. Ist $x = (\infty^{(a)}, a, -a, 0)$, so ist die Differenz $x_i - x_j$ genau dann definiert, wenn $i, j \neq 0$. Daher ergeben die Differenzen

$x_{\alpha i} - x_{\alpha j}$ gerade die Werte $\pm a$, falls (i, j) aus der ersten oder zweiten Bahn, und $\pm 2a$, falls (i, j) aus der dritten Bahn ist. Wenn a die Zahlen $1, 2, \ldots, m$ durchläuft, ergeben sich also jedesmal alle Elemente $\neq 0$ genau einmal. Daher gilt auch (S2'). Also ist Q^* Starter.

4.2.8. *Folgerung.* Existiert ein $(m, 4, 1; V_4)$-SBTS, so existiert auch ein $(3m + 1, 4, 1; V_4)$-SBTS.

Beweis Wende Satz 4.2.6. auf den eben konstruierten unvollständigen Starter an.

Die folgenden unvollständigen Starter stammen von Wilson [32]:

4.2.9. *Beispiele.* H^4 sei die Gruppe der vierten Potenzen in $GF(q)$, $q = 4f + 1$. Unvollständige $GF(q) \times H^4$-Starter für ein $((4f + 1) + f, 6, 1; Z_6)$-SBTS sind

(i) $\{(\infty, 0, 1, 3, 7, 9)\}$ $(q = 29, f = 7)$,

(ii) $\{(\infty, 1, 13, 21, 14, 34)\}$ $(q = 37, f = 9)$.

4.3. Rekursive Konstruktionen

Die einfachste, für den Existenzbeweis in Kapitel 5 aber grundlegende, rekursive Konstruktion für SBTS ist:

4.3.1. *PBD-Konstruktion.* $(P, \mathcal{B})$ sei ein PBD vom Index 1. Für jeden Block $B \in \mathcal{B}$ sei Q_B ein $(B, k, \mu, M; G)$-SBTS. Dann ist das Tupelsystem

$$Q = \bigcup_{B \in \mathcal{B}} Q_B \tag{1}$$

(wo die Tupel entsprechend ihrer Vielfachheiten gezählt werden) ein $(P, k, \mu, M; G)$-SBTS.

Wir erinnern daran, daß die Schreibweise P für den Parameter v besagen soll, daß die Punktmenge P ist, und $v = |P|$.

Beweis von 4.3.1. Wir berechnen die Situationszahlen $\rho_i(a)$ und $\mu_{ij}(a, b)$, $(i \neq j, a \neq b)$. $\rho_i(a)$ ist die Zahl der Tupel $x \in Q$ mit $x_i = a$. Ein solches Tupel kann höchstens in einem Q_B mit $a \in B$ liegen. Daher ist, unter Verwendung von 2.3.6. (2) mit $\lambda = 1$,

$$\rho_i(a) = \sum_{a \in B \in \mathcal{B}} \rho_i^{Q_B}(a) = \sum_{a \in B \in \mathcal{B}} \mu(|B| - 1) = \mu(|P| - 1).$$

$\mu_{ij}(a, b)$ ist die Zahl der Tupel $x \in Q$ mit $x_i = a$, $x_j = b$. Ein solches Tupel kann nur in dem eindeutig bestimmten Q_B liegen, wo B der a und b verbindende Block ist. Daher ist $\mu_{ij}(a, b) = \mu_{ij}^{Q_B}(a, b) \in \{0, \mu_{ij}\}$. Also gilt (SBTS3).

(SBTS1) und (SBTS2) übertragen sich ohne weiteres.

Wesentlich für die Anwendungen ist, daß die PBD-Konstruktion

(ebenso wie eine Reihe weiterer rekursiver Konstruktionen) die freie Automorphismengruppe erhält. Reine Automorphismen bleiben i.a. dagegen nicht erhalten.

Für HTS tritt an die Stelle der PBD-Konstruktion eine Konstruktion, die GDD verwendet. Für diese Konstruktion werden jedoch auch SBTS gebraucht.

4.3.2. *GDD-Konstruktion.* $(P, \mathcal{G}, \mathcal{B})$ sei ein GDD vom Index 1. Für jeden Block $B \in \mathcal{B}$ sei Q_B ein $(B, k, \mu; G)$-SBTS. Für jede Gruppe $A \in \mathcal{G}$ sei Q_A ein $(A, k, \mu; G)$-HTS. Dann ist

$$Q = \bigcup_{B \in \mathcal{B}} Q_B \cup \bigcup_{A \in \mathcal{G}} Q_A \tag{2}$$

ein $(P, k, \mu; G)$-HTS.

Beweis. Wieder überträgt sich die Automorphismengruppe. Wir berechnen die Situationszahlen $\mu_{ij}(a, b)$, $i \neq j$.

$\mu_{ij}(a, b)$ ist die Zahl der Tupel $x \in Q$ mit $x_i = a$, $x_j = b$. Liegen nun a und b in derselben Gruppe A, so kann ein solches Tupel nur in Q_A liegen. Daher ist dann $\mu_{ij}(a, b) = \mu_{ij}^{Q_A}(a, b) = \mu$. Liegen aber a und b in verschiedenen Gruppen, so gibt es genau einen Block B, der a und b enthält, und die gesuchten Tupel müssen in Q_B liegen. Dann ist also $\mu_{ij}(a, b) = \mu_{ij}^{Q_B}(a, b) = \mu$. Daher ist Q ein $(P, k, \mu; G)$-HTS.

Wir geben nun noch eine Konstruktion für HTS an, bei der die Parameter k und μ vergrößert werden, v dafür konstant bleibt.

4.3.3. *Satz.* (P, I, Q, ϵ) sei ein (v, k, μ)-HTS, und $(P, I_0, Q_0, \epsilon_0)$ sei ein $(v, k_0 + 1, 1)$-HTS. Ist $\infty \in I_0$ ein festes Element, und $I' = I_0 - \{\infty\}$, so ist das Tupelsystem $(P, I \times I' \cup \{\infty\}, Q \times P, \epsilon^*)$ mit

$$\epsilon^*((x, c), (i, j)) \equiv (x, c)_{i,j} = z_j, \quad \text{wo } z \in Q_0, \quad z_0 = x_i, \quad z_\infty = c, \tag{3}$$

$$\epsilon^*((x, c), \infty) \equiv (x, c)_\infty = c, \tag{4}$$

ein $(v, kk_0 + 1, v\mu)$-HTS. 0 ist dabei eine feste Stelle von I.

Beweis. Wir bemerken zunächst, daß das Tupel z in (3) eindeutig bestimmt ist; also ist die Belegung ϵ^* wohldefiniert. Zur Berechnung der Situationszahlen unterscheiden wir zwei Fälle.

Fall 1 :

$$(x, c)_\infty = a, (x, c)_{i,j} = b \tag{5}$$

gilt genau dann, wenn $c = a$, $x_i = z_0$, $z_j = b$, $z_\infty = c$. Daher ist für gegebene i, j, a, b das Tupel $z \in Q_0$ eindeutig durch $z_j = b$, $z_\infty = c$ bestimmt; c ist bestimmt durch $c = a$, und $x_i = z_0$ hat μv Lösungen $x \in Q$. Daher hat (5) genau μv Lösungen $(x, c) \in Q \times P$.

Fall 2 :

$$(x, c)_{i,j} = a, (x, c)_{i',j'} = b, (i, j) \neq (i', j') \tag{6}$$

gilt genau dann, wenn $x_i = z_0$, $x_{i'} = z_0'$, $z_j = a$, $z_\infty = c$, $z_{j'}' = b$, $z_\infty' = c$. Ist nun $i \neq i'$, so sind für jedes $c \in P$ die Tupel z, $z' \in Q_0$ eindeutig bestimmt durch $z_j = a$, $z_\infty = c$, bzw. $z_{j'}' = b$, $z_\infty' = c$. Mit diesen z, z' hat dann $x_i = z_0$, $x_{i'} = z_0'$ genau μ Lösungen $x \in Q$. Insgesamt hat dann (6) genau $\mu\nu$ Lösungen $(x, c) \in Q \times P$.

Ist aber $i = i'$, $j \neq j'$, so folgt aus $z_0 = z_0' = x_i$, $z_\infty = z_\infty' = c$ zunächst $z' = z$, und z ist dann durch $z_j = a$, $z_{j'} = z_{j'}' = b$ eindeutig bestimmt. Mit diesem z ist dann $c = z_\infty$ festgelegt. Schließlich läßt $x_i = z_0$ $\mu\nu$ Möglichkeiten für x übrig. Daher gibt es wieder genau $\mu\nu$ Lösungen $(x, c) \in Q \times P$ von (6).

Also sind in jedem Fall die Situationszahlen gleich $\mu\nu$. Daraus ergibt sich die Behauptung.

Bemerkung. Wir weisen darauf hin, daß diese Konstruktion gemeinsame reine Automorphismen der beiden Tupelsysteme erhält (freie dagegen i.A. nicht).

4.3.4. *Folgerung.* ν sei eine natürliche Zahl, zu der es ein $(1, \nu)$-ARBIBD (d.h. eine affine Ebene der Ordnung ν) gibt, also z.B. eine Primzahlpotenz. Dann folgt aus der Existenz eines (μ, ν)-ARBIBD die Existenz eines $(\nu\mu, \nu)$-ARBIBD.

Beweis. Die Existenz von $(1, \nu)$-ARBIBDs wurde in 4.1.7. bewiesen.— Setzt man in Satz 4.3.3. $k = \dfrac{\mu\nu^2 - 1}{\nu - 1}$, $k_0 = \nu$, so ist $kk_0 = \dfrac{\mu\nu^3 - 1}{\nu - 1}$. D.h., wenn Q und Q_0 maximal sind, so ist auch Q maximal. Die Behauptung ergibt sich nun unmittelbar aus Satz 3.2.8. (c).

5. EXISTENZSÄTZE FÜR GROSSE ν

Hier werden asymptotische Aussagen über die Existenz von SBTS gemacht (Daraus ergeben sich nach Satz 2.2.7. entsprechende HTS!). Grundlage dafür sind zwei Sätze von Wilson über Kreisteilungszahlen (Satz 5.1.1.) und die Existenz von PBD (Satz 2.3.5.).

In den Abschnitten 5.1. und 5.3. werden für alle genügend große Primzahlpotenzen Starter *bzw.* unvollständige Starter zu $GF(q)$ konstruiert. Die zugehörigen SBTS dienen als Ausgangspunkt für den Beweis der beiden Existenzsätze 5.2.7. und 5.4.6. Satz 5.4.6. zeigt, daß in (wichtigen) Spezialfällen die notwendigen Bedingungen aus Abschnitt 2.2. für genügend große ν auch hinreichend sind. Die allgemeine diesbezügliche Vermutung konnte nicht bewiesen werden.

5.1. Starter in Endlichen Körpern

$q = ef + 1$ (e gerade, f ungerade) sei eine Primzahlpotenz, und $K = GF(q)$ sei der endliche Körper mit q Elementen. H^e sei die Gruppe der e-ten Potenzen in $K^\times$. H^e enthält f Elemente. Ist ϵ ein (im folgenden festes)

primitives Element von K, so bezeichnen wir die Nebenklassen von H^e als

$$H_s^e = \{\epsilon^{ei+s} \mid i = 0, \ldots, f-1\}, s \bmod e.$$

Setzen wir nun $s^* = s + \frac{e}{2}$, so gilt

$$s^{**} = s,\ s^* \neq s,\ -H_s^e = H_s^e{}^* \text{ für alle } s \bmod e. \tag{1}$$

Für jedes k-Tupel x mit lauter verschiedenen Einträgen aus K setzen wir

$$c_{ij}(x) = s \Leftrightarrow (x_i - x_j)\, H^e = H_s^e \quad (i, j \in I, i \neq j). \tag{2}$$

Die Existenzsätze dieses Kapitels beruhen entscheidend auf dem folgenden Satz, für dessen Beweis wir auf Wilson [27] verweisen.

5.1.1. *Satz (Wilson).* Es seien c_{ij} $(i, j \in I, i \neq j)$ irgendwelche Restklassen modulo e, die der Bedingung

$$c_{ji} = c_{ij}^* \text{ für alle } i \neq j \tag{3}$$

genügen. Ist dann $q > e^{k(k-1)}$, so gibt es mindestens ein k-Tupel x mit lauter verschiedenen Einträgen aus $GF(q)$, derart, daß

$$c_{ij}(x) = c_{ij} \text{ für alle } i, j \in I, i \neq j. \tag{4}$$

Bemerkung. (3) ist notwendig für (4); daher ist der Satz (für große q) bestmöglich.

5.1.2. *Satz.* G sei eine auf der k-Menge I treue Permutationsgruppe, und $M = (\mu_{ij})$ sei eine symmetrische $k \times k$-Matrix mit ganzzahligen Einträgen, die die folgenden Bedingungen erfüllt:

$$\mu_{ii} = 0,\ \mu_{ij} \geqslant \mu > 0 \text{ für } i \neq j, \tag{5a}$$

$$\mu_{\alpha i, \alpha j} = \mu_{ij} = \mu_{ji} \text{ für } \alpha \in G, \tag{5b}$$

$$|G_{ij}| \mid \mu_{ij} \text{ für alle } i \neq j. \tag{5c}$$

Angenommen, es ist

$$q = ef + 1 > e^{k(k-1)} \text{ eine Primpotenz}, \tag{6a}$$

$$e \text{ gerade}, f \text{ ungerade}, \tag{6b}$$

$$\mu_{ij} \mid e\mu \text{ für alle } i \neq j, \tag{6c}$$

$$|G| \mid e\mu. \tag{6d}$$

Dann existiert ein $(q, k, \mu, M; G)$-SBTS.

Beweis. Wir beweisen die Existenz eines $GF(q) \times H^e$-Starters für ein $(q, k, \mu, M; G)$-SBTS. Die Behauptung folgt dann sofort aus Satz 4.2.2. Da der Beweis den nichtkonstruktiven Satz 5.1.1. verwendet, kann kein Konstruktionsverfahren für den Starter (und damit das SBTS) angegeben werden.

(a) R sei eine Menge mit

$$|R| = |G|^{-1} e\mu. \tag{7}$$

H sei die von den Permutationen $\alpha : (i, j) \to (\alpha i, \alpha j)$, $\alpha \in G$, und $* : (i, j) \to (j, i)$ erzeugte Permutationsgruppe auf $I \times I$. Γ sei eine Bahn von H, die ein Paar (s, t) mit $s \neq t$ enthält. Wir setzen $X_\Gamma = \Gamma \times R$. Dann ist $|X_\Gamma| = |\Gamma| \cdot |R| = \frac{|H|}{|H_{(s,t)}|} \cdot \frac{e\mu}{|G|}$, wegen $|H| = 2 \cdot |G|$ also

$$|X_\Gamma| = \frac{2e\mu}{|H_{(s,t)}|} . \tag{8}$$

(b) Es sei nun $E = \left\{0, 1, \ldots, \frac{e}{2} - 1\right\}$, $E^* = \left\{\frac{e}{2}, \frac{e}{2} + 1, \ldots, e - 1\right\}$. Wir unterscheiden mehrere Fälle.

Fall 1. $G(s, t) \neq G(t, s)$. In diesem Fall ist $|H_{(s,t)}| = |G_{st}|$, und nach (5c) und (8) ist

$$\left(\frac{e\mu}{\mu_{st}}\right)^{-1} \cdot \frac{1}{2} |X_\Gamma| = \frac{\mu_{st}}{|G_{st}|} \quad \text{ganzzahlig.} \tag{9}$$

Wir setzen jetzt

$$Z_\Gamma = \{(i, j, t) \in X_\Gamma \mid (i, j) \in G(s, t)\}, \tag{10a}$$

$$Z_\Gamma^* = \{(i, j, t) \in X_\Gamma \mid (i, j) \in G(t, s)\}. \tag{10b}$$

Die Zahl $\frac{e\mu}{\mu_{st}}$ ist nach (6c) ganz und nach (5a) kleiner oder gleich e. Daher kann man Z_Γ in e Mengen $T_{\Gamma l}$, $l \in E \cup E^*$ der Länge $\frac{\mu_{st}}{|G_{st}|}$ oder 0 zerlegen. Die Mengen

$$T_{\Gamma t}^* = \{(i, j, i) \mid (j, i, t) \in T_{\Gamma l}\}, \; l \in E \cup E^*, \tag{11}$$

zerlegen dann Z_Γ^* in Mengen der Länge $\frac{\mu_{st}}{|G_{st}|}$ oder 0.

Fall 2: $G(s, t) = G(t, s)$. Jetzt ist $|H_{(s,t)}| = 2 \cdot |G_{st}|$, und $|\Gamma|$, also auch $|X_\Gamma|$, ist gerade. Nach (8) ist

$$|X_\Gamma| = \frac{\mu_{st}}{|G_{st}|} \cdot \frac{e\mu}{\mu_{st}} , \tag{12}$$

und nach (5a), (5c) und (6c) sind beide Faktoren ganz, und $\frac{e\mu}{\mu_{st}} \leqslant e$. Wir zerlegen nun Γ irgendwie in zwei Teilmengen Γ', Γ'^*, so daß $(i, j) \in \Gamma'^* \Leftrightarrow (j, i) \in \Gamma'$, und setzen

$$Z_\Gamma = \{(i, j, t) \in X_\Gamma \mid (i, j) \in \Gamma'\}, \tag{13a}$$

$$Z_\Gamma^* = \{(i, j, t) \in X_\Gamma \mid (i, j) \in \Gamma'^*\}. \tag{13b}$$

Fall 2a: Ist nun $\frac{e\mu}{\mu_{st}}$ gerade, so kann man wegen $|Z_\Gamma| = \frac{1}{2} |X_\Gamma|$ die Menge

Z_Γ in $\frac{e}{2}$ Mengen $T_{\Gamma l}$, $l \in E$, der Länge $\frac{\mu_{st}}{|G_{st}|}$ oder 0 zerlegen. Wir setzen außerdem $T_{\Gamma l} = \emptyset$ für $l \in E^*$, und definieren $T^*_{\Gamma l}$ wieder durch (11).

Fall 2b: Ist aber $\frac{e\mu}{\mu_{st}}$ ungerade, so muß $\frac{\mu_{st}}{|G_{st}|}$ gerade sein, und man kann Z_Γ in e Mengen $S_{\Gamma l}$, $l \in E \cup E^*$, der Länge $\frac{\mu_{st}}{2|G_{st}|}$ oder 0 zerlegen. Setze nun

$$S^*_{\Gamma l} = \{(i, j, t) \mid (j, i, t) \in S_{\Gamma l}\}, \tag{14}$$

$$T_{\Gamma l} = T^*_{\Gamma l} = S_{\Gamma l} \cup S^*_{\Gamma l}. \tag{15}$$

Dann bilden die $T_{\Gamma l}$ eine Partition von X_Γ in Mengen der Länge $\frac{\mu_{st}}{|G_{st}|}$ oder O.

(c) Angenommen, es sei $(i, j, t) \in I \times I \times R$, $i \neq j$. Nach unsrer Konstruktion ist die Zahl

$$c_{ij}(t) = l \Leftrightarrow (i, j, t) \in T_{\Gamma l} \cup T^*_{\Gamma l}, \quad \Gamma = H(i, j),$$

eindeutig bestimmt. Wegen (11) bzw. (15) erfüllen die $c_{ij}(t)$ die Bedingung (2). Wegen (6a), (6b) können wir daher Satz 5.1.1. anwenden und erhalten für jedes $t \in R$ die Existenz eines k-Tupels x^t mit lauter verschiedenen Einträgen aus $K = GF(q)$ mit der Eigenschaft

$$c_{ij}(x^t) = c_{ij}(t) \text{ für alle } i \neq j. \tag{16}$$

Schließlich setzen wir

$$Q^* = \{x^t \mid t \in R\}.$$

(d) Wir zeigen, daß Q^* ein $K \times H^e$-Starter für ein $(q, k, \mu, M; G)$-SBTS ist. Dazu sei, für $a \in K^\times$, μ_{ija} die Zahl der $(x, \alpha) \in Q^* \times G$ mit

$$H^e(x_{\alpha i} - x_{\alpha j}) = H^e a. \tag{17}$$

Es sei $i \neq j$, $a \neq 0$, $a \in H^e$. Für alle $x \in Q$ gibt es genau ein $t \in R$ mit $x = x^t$. Daher ist (1) $\Leftrightarrow c_{\alpha i, \alpha j}(x) = l \Leftrightarrow c_{\alpha i, \alpha j}(t) = l \Leftrightarrow (\alpha i, \alpha j, t) \in T_{\Gamma l} \cup T^*_{\Gamma l}$, wo $\Gamma = H(\alpha i, \alpha j) = H(i, j)$.

Fall 1. $G(i, j) \neq G(j, i)$, (s, t) sei das Paar, das oben zur Konstruktion der Zerlegung von X_Γ verwendet wurde. Dann ist (17) äquivalent zu

$$(\alpha i, \alpha j, t) \in T_{\Gamma l}, \tag{18a}$$

wenn $(i, j) \in G\,(s, t)$, und zu

$$(\alpha i, \alpha j, t) \in T^*_{\Gamma l}, \tag{18b}$$

wenn $(i, j) \in G(t, s)$.

Fall 2. $G(i, j) = G(j, i)$. Dann ist (17) wieder äquivalent zu (18a),

wenn $l \in E$, und zu (18b), wenn $l \in E^*$.†

Nun ist die Anzahl der Tripel in $T_{\Gamma l}$ bzw. $T^*_{\Gamma l}$ entweder 0 oder $\frac{\mu_{st}}{|G_{st}|} = \frac{\mu_{ij}}{|G_{ij}|}$ wegen (5b), und für jedes solche Tripel (i_0, j_0, t_0) ist die Zahl der Lösungen von $(\alpha i, \alpha j, t) = (i_0, j_0, t_0)$ gleich $|G_{ij}|$. Daher gilt $\mu_{ija} \in \{0, \mu_{st}\}$. Also ist (S2) erfüllt. (S0) gilt nach Konstruktion der x^t, und (S1) folgt aus $|Q^*| = |R|$ und (7). Damit ist der Satz bewiesen.

5.2. Der Schwache Existenzsatz Für SBTS

In diesem Abschnitt sei $k \geqslant 3$, $\mu \geqslant 1$. Wir benutzen die Schreibweise $B_k(\mu, M; G)$ bzw. $B_k(\mu; G)$ für die Menge aller natürlichen Zahlen v, für die ein $(v, k, \mu, (M); G)$-SBTS existiert.

Unsere Existenzaussagen beruhen im wesentlichen auf den Sätzen 5.1.2., 4.3.1., und 2.3.5.

5.2.1. *Lemma.* $B_k(\mu, M; G)$ und $B_k(\mu; G)$ sind PBD-abgeschlossene Mengen.

Beweis. Angesichts der PBD-Konstruktion 4.3.1. folgt das sofort aus der Definition der PBD-abgeschlossenen Mengen (2.3.4.).

5.2.2. *Lemma.* Es gibt natürliche Zahlen $\alpha = \alpha_k(\mu, M; G)$, $\beta = \beta_k(\mu, M; G)$ derart, daß $B_k(\mu, M; G)$ eine kofinale Teilmenge ist von

$$H^\alpha_\beta = \{v \in \mathbb{N} \mid \alpha \mid v - 1, \beta \mid v(v-1)\}. \tag{1}$$

Beweis. Wir wenden Satz 2.3.5. auf die (nach dem vorigen Lemma PBD-abgeschlossene) Menge $B_k(\mu, M; G)$ an. Die Zahlen α, β ergeben sich als

$$\alpha_k(\mu, M; G) = \operatorname*{ggT}_{v \in B_k(\mu, M; G)} (v - 1), \tag{2}$$

$$\beta_k(\mu, M; G) = \operatorname*{ggT}_{v \in B_k(\mu, M; G)} (v(v-1)). \tag{3}$$

5.2.3. *Lemma.* (a) Für jede mögliche Parameterkombination ist

$$1 \in B_k(\mu, M; G). \tag{4}$$

(b) $B_k(\mu, M; G) = \{1\}$, außer wenn gilt:

$$\mu_{ii} = 0, \mu_{ij} \geqslant \mu > 0 \text{ für } i \neq j, \tag{5a}$$

$$\mu_{\alpha i, \alpha j} = \mu_{ij} = \mu_{ji} \text{ für } \alpha \in G, \tag{5b}$$

$$|G_{ij}| \mid \mu_{ij} \text{ für alle } i \neq j. \tag{5c}$$

Beweis. (a) Die leere Menge ist ein $(1, k, \mu, M; G)$-SBTS über jeder 1-Menge P, für jede Parameterkombination. (b) ist eine Folge von (a) und Proposition 2.2.2.

† (Wegen $T_{\Gamma l} = T^*_{\Gamma l}$ gilt das auch im Fall 2*b*!)

5.2.4. *Lemma.* Angenommen, es ist

$$q = ef + 1 \text{ eine Primzahlpotenz, } q > e^{k(k-1)}, \tag{6a}$$

$$e \text{ gerade, } f \text{ ungerade,} \tag{6b}$$

$$\mu_{ij} \mid e\mu \text{ für alle } i \neq j, \tag{6c}$$

$$|G| \mid e\mu. \tag{6d}$$

Gelten dann (5a), (5b) und (5c), so ist

$$q \in B_k(\mu, M; G).$$

Beweis. Wende Satz 5.1.2. an.

Wir betrachten nun eine feste, $(5a - c)$ erfüllende Parameterkombination $(k, \mu, M; G)$ und definieren die Zahlen

$$\mu^* = \underset{i,j \in I,\, i \neq j}{\text{kgV}} (\mu_{ij}), \tag{7}$$

$$e_0 = \frac{\mu^*|G|}{\text{ggT}(\mu^*|G|, \mu|G|, \mu\mu^*)}. \tag{8}$$

Dabei bezeichnet kgV das kleinste gemeinsame Vielfache, und ggT den größten gemeinsamen Teiler der nachfolgenden Elemente. Mit e bezeichnen wir das kleinste gerade Vielfache von e_0.

5.2.5. *Lemma.* Ist q eine Primzahlpotenz mit

$$q \equiv e + 1 \mod 2e, \tag{9}$$

$$q > e^{k(k-1)}, \tag{10}$$

so ist $q \in B_k(\mu, M; G)$.

Beweis. Aus (7) und (8) ergibt sich, daß $\frac{e_0\mu}{|G|} = \frac{\mu\mu^*}{\text{ggT}(\mu^*|G|, \mu|G|, \mu\mu^*)}$ und $\frac{e_0\mu}{\mu_{ij}} = \frac{\mu^*}{\mu_{ij}} \cdot \frac{\mu|G|}{\text{ggT}(\mu^*|G|, \mu|G|, \mu\mu^*)}$ ganze Zahlen sind. Daher ist $|G| \mid e_0\mu$, $\mu_{ij} \mid e_0\mu$, und wegen $e_0 \mid e$ folgen (6c), (6d). Nach Konstruktion ist e gerade, und mit $f = \frac{q-1}{e}$ ergeben sich wegen (9) auch (6a) und (6b). Wenden wir nun Lemma 5.2.4. an, so erhalten wir das gewünschte Resultat.

5.2.6. *Satz.* Gelten $(5a - c)$, so ist $\beta_k(\mu, M; G)$ das kleinste gerade Vielfache von

$$e_0 = \frac{\mu^*|G|}{\text{ggT}(\mu^*|G|, \mu|G|, \mu\mu^*)}.$$

Dabei ist

$$\mu^* = \underset{i,j \in I, i \neq j}{\text{kgV}} (\mu_{ij}).$$

Beweis. Wegen (7), (8) müssen wir $\beta_k(\mu, M; G) = e$ zeigen. Nach Dirichlets Satz über Primzahlen in arithmetischen Progressionen (s. etwa

Prachar [20]) gibt es für teilerfremde Zahlen a, m unendlich viele Primzahlen $p \equiv a \bmod m$. Insbesondere gibt es Primzahlen p, q mit

$$p \equiv 1 + e \bmod 2e(e-1),\ p > e^{k(k-1)}, \tag{11}$$

$$q \equiv 1 - e \bmod 2p(p-1),\ q > e^{k(k-1)}. \tag{12}$$

Für solche Primzahlen p, q ist $p, q \equiv 1 + e \bmod 2e$. Nach Lemma 5.2.5. ist daher $p, q \in B_k(\mu, M; G)$. Wegen $\mathrm{ggT}(p(p-1), q(q-1)) = \mathrm{ggT}(p(p-1), e(e-1)) = \mathrm{ggT}(e(e+1), e(e-1)) = e \cdot \mathrm{ggT}(e+1, e-1) = e$ (e ist gerade!) ergibt sich aus (3) dann $\beta_k(\mu, M; G) \mid e$.

Ist andrerseits $v \in B_k(\mu, M; G)$, $v > 1$, so ist nach Proposition 2.2.2. $\mu^* \mid \mu(v-1), |G| \mid \mu v(v-1)$, also

$$\mu^*|G| \mid \mathrm{ggT}(\mu^*|G|, \mu|G|, \mu^*\mu)v(v-1).$$

Daher ist $e_0 \mid v(v-1)$, und weil $v(v-1)$ gerade ist, sogar $e \mid v(v-1)$. Da dies für alle $v \in B_k(\mu, M; G)$ gilt, folgt $e \mid \beta_k(\mu, M; G)$. Daher ist $\beta_k(\mu, M; G) = e$.

Als Folgerung aus Satz 5.2.6. können wir nun einen ersten Existenzsatz erhalten. Proposition 2.2.2. enthält die notwendigen Bedingungen für SBTS. Wir setzen davon nur (5a–c) voraus und erhalten dementsprechend eine schwächere Existenzaussage. Immerhin wird jedoch dadurch die Existenz von SBTS für genügend große v auf die Konstruktion endlich vieler Beispiele zurückgeführt.

5.2.7. *Schwacher Existenzsatz für SBTS.* Es sei $k \geqslant 2$, $\mu \geqslant 1$. Gelten

$$\mu_{ii} = 0,\ \mu_{ij} \geqslant \mu > 0 \text{ für } i \neq j, \tag{5a}$$

$$\mu_{\alpha i, \alpha j} = \mu_{ij} = \mu_{ji} \text{ für } \alpha \in G, \tag{5b}$$

$$|G_{ij}| \mid \mu_{ij} \text{ für alle } i \neq j, \tag{5c}$$

und ist $\beta_k(\mu, M; G)$ das kleinste gerade Vielfache von

$$e_0 = \frac{\mu^*|G|}{\mathrm{ggT}(\mu^*|G|, \mu|G|, \mu\mu^*)},$$

so existiert eine natürliche Zahl $v_k^*(\mu, M; G)$ derart, daß gilt: Existiert ein $(v_0, k, \mu, M; G)$-SBTS, und ist

$$v \equiv v_0 \bmod \beta_k(\mu, M; G),\ v \geqslant v_k^*(\mu, M; G),$$

so existiert auch ein $(v, k, \mu, M; G)$-SBTS.

Insbesondere existiert ein $(v, k, \mu, M; G)$-SBTS für jede genügend große natürliche Zahl $v \equiv 1 \bmod \beta_k(\mu, M; G)$.

Beweis. Der erste Teil ist eine einfache Folgerung aus den Tatsachen, daß $B_k(\mu, M; G)$ eine kofinale Teilmenge von H_β^α ist (Lemma 5.2.2.), und daß H_β^α mit einem v_0 alle $v \equiv v_0 \bmod \beta$ enthält. Der zweite Teil folgt daraus wegen (4).

Bemerkung. Es ist interessant, daß also für jede theoretisch denkbare

freie Automorphismengruppe G unendlich viele SBTS mit dieser Gruppe existieren!

5.3. Unvollständige Starter

Wir übernehmen die Bezeichnungen der Abschnitte 4.2. und 5.1.

5.3.1. *Satz.* G sei eine auf der k-Menge I treue Permutationsgruppe, und es sei

$$|G_i| \mid \mu \quad \text{für alle } i \in I. \tag{1}$$

Ist dann mit

$$e = \mu^{-1} |G| w + r(k-2) \tag{2}$$

$$e \text{ gerade}, f \text{ ungerade}, \tag{3a}$$

$$q = ef + 1 > e^{k(k-1)} \text{ eine Primzahlpotenz}, \tag{3b}$$

und existiert ein $(rf, k, \mu; G)$-SBTS, so existiert auch ein $(q + rf, k, \mu; G)$-SBTS.

Beweis. Wir beweisen die Existenz eines unvollständigen $GF(q) \times H^e$-Starters für ein $(q + rf, k; \mu; G)$-SBTS. Die Behauptung folgt dann sofort aus Satz 4.2.6. Der Beweis verläuft analog zum Beweis von Satz 5.1.2.; daher führen wir nur die wesentlich davon abweichenden Schritte näher aus.

(a) S sei ein Repräsentantensystem der G-Bahnen von I. $R^{(0)}$, $R_i^{(\nu)}$ $(i \in S, \nu = 1, \ldots, r)$ seien paarweis disjunkte Mengen mit

$$|R^{(0)}| = w, \; |R_i^{(\nu)}| = |G_i|^{-1}\mu \quad (i \in S, \nu = 1, \ldots, r). \tag{4}$$

Wir setzen

$$R^* = \bigcup_{i \in S} \bigcup_{\nu=1}^{r} R_i^{(\nu)} \cup R^{(0)}. \tag{5}$$

H sei dieselbe Gruppe wie im Beweis von 5.1.2., und Γ sei eine Bahn von H, die ein Paar (s, t) mit $s \neq t$ enthält. Wir setzen

$$\Delta_{i_0} = \{(i, j) \in \Gamma \mid i = i_0 \text{ oder } j = i_0\}, \; i_0 \in S, \tag{6}$$

$$X_\Gamma = \bigcup_{i \in S} \bigcup_{\nu=1}^{r} (\Gamma - \Delta_i) \times R_i^{(\nu)} \cup \Gamma \times R^{(0)}. \tag{7}$$

Um die Mächtigkeit von X_Γ bestimmen zu können, bemerken wir zunächst, daß

$$|H_{(s,t)}| \cdot |\Gamma| = |H| = 2\,|G|. \tag{8}$$

Wir zählen nun die Zahl h_i der $\alpha \in H$ mit $\alpha(s, t) \in \Delta_i$ auf zweifache Weise *ab*. Halten wir zuerst Δ_i fest, so ergeben sich für jedes Paar $\in \Delta_i$ genau $|H_{(s,t)}|$ Lösungen, also ist $h_i = |H_{(s,t)}| \cdot |\Delta_i|$. Andrerseits ist $\alpha(s, t) \in \Delta_i, \alpha \in G \Leftrightarrow \alpha s = i$ oder $\alpha t = i$, und in diesem Fall ist auch $\alpha(s, t) \in \Delta_i$. Ist daher

$$\delta_i = |Gi \cap \{s, t\}|, \tag{9}$$

so ist $h_i = 2\,|G_i|\delta_i$. Also ist

$$|H_{(s,t)}| \cdot |\Delta_i| = 2|G_i|\delta_i. \tag{10}$$

Aus (9) ergibt sich noch

$$\sum_{i \in S} \delta_i = 2. \tag{11}$$

Wenden wir nun der Reihe nach (7), (4), (10), (2) und (8) an, so erhalten wir

$$\begin{aligned} X_\Gamma &= \sum_{i \in S} \sum_{\nu=1}^{r} (|\Gamma| - |\Delta_i|)\, |R_i^{(\nu)}| + |\Gamma|\, |R^{(0)}| \\ &= |\Gamma| \cdot \Big(\sum_{i \in S} \sum_{\nu=1}^{r} |R_i^{(\nu)}| + |R^{(0)}| \Big) - \sum_{i \in S} \sum_{\nu=1}^{r} |\Delta_i|\, |R_i^{(\nu)}| \\ &= |\Gamma| \cdot \Big(\sum_{i \in S} \frac{\mu r}{|G_i|} + w \Big) - \sum_{i \in S} \frac{|\Delta_i| r\mu}{|G_i|} \\ &= \frac{|\Gamma|\mu}{|G|} \Big(r \sum_{i \in S} \frac{|G|}{|G_i|} + \frac{|G| w}{\mu} \Big) - \frac{2r\mu}{|H_{(s,t)}|} \sum_{i \in S} \delta_i \\ &= \frac{2\mu}{|H_{(s,t)}|} (rk + e - r(k-2)) - \frac{4r\mu}{|H_{(s,t)}|} = \frac{2e\mu}{|H_{(s,t)}|}. \end{aligned}$$

Daher gilt, wie in 5.1.2.,

$$|X_\Gamma| = \frac{2e\mu}{|H_{(s,t)}|}. \tag{12}$$

(b) Es ist jetzt $\mu_{ij} = \mu$ für alle $i \neq j$. Beachtet man dies, so erhält man auf dieselbe Weise wie in 5.1.2. im Fall 1 eine Partition von X_Γ in $2e$ Mengen $T_{\Gamma l}$, $T^*_{\Gamma l} (l \in E \cup E^*)$ der Länge $\frac{\mu}{|G_{st}|}$, und im Fall $2a$ eine Partition von X_Γ in e Mengen $T_{\Gamma l}$, $T^*_{\Gamma l} (l \in E)$ der Länge $\frac{\mu}{|G_{st}|}$ (dann setzen wir wieder $T_{\Gamma l} = T^*_{\Gamma l} = \phi$ für $l \in E^*$). Da e gerade ist, kann der Fall $2b$ jetzt nicht mehr auftreten.

(c) Wir definieren nun für $(i, j, t) \in I \times I \times R^{(0)}$, $i \neq j$, oder für $(i, j, t) \in I \times I \times R_s^{(\nu)}$, $s \neq i \neq j \neq s$, $s \in I$, $\nu = 1, \ldots, r$,

$$c_{ij}(t) = l \Leftrightarrow (i, j, t) \in T_{\Gamma l} \cup T^*_{\Gamma l}, \quad \Gamma = H(i, j),$$

und erhalten für jedes $t \in R$ ein Schema $c_{ij}(t)$, das die Voraussetzung von Satz 5.1.1. erfüllt (für $t \in R^{(0)}$ mit I, für $t \in R_s^{(\nu)}$ mit $I - \{s\}$ als Stellenmenge). Daher existieren

(i) für jedes $t \in R^{(0)}$ ein k-Tupel x^t mit lauter verschiedenen Einträgen aus K mit der Eigenschaft

$$c_{ij}(x^t) = c_{ij}(t) \text{ für } i \neq j, \tag{13}$$

(ii) für jedes $t \in R_s^{(\nu)}$ $(s \in S, \nu = 1, \ldots, r)$ ein k-Tupel x^t mit lauter

verschiedenen Einträgen aus K mit der Eigenschaft

$$x_s^t = \infty^{(\nu)}, \quad c_{ij}(x^t) = c_{ij}(t) \text{ für } s \neq i \neq j \neq s. \tag{14}$$

Im zweiten Fall haben wir die von Satz 5.1.1. nicht "gefüllte" Stelle s mit $\infty^{(\nu)}$ besetzt. Wir setzen nun

$$Q^{(0)} = \{x^t \mid t \in R^{(0)}\}, \tag{15a}$$

$$Q_s^{(\nu)} = \{x^t \mid t \in R_s^{(\nu)}\} \quad (s \in S, \nu = 1, \ldots, r). \tag{15b}$$

(d) Ebenso wie in 5.1.2. zeigt man nun, daß

$$Q^* = \bigcup_{s \in S} \bigcup_{\nu=1}^{r} Q_s^{(\nu)} \cup Q^{(0)}$$

ein unvollständiger $K \times H^e$-Starter für ein $(q + rf, k, \mu; G)$-SBTS ist. Zu beachten ist nur, daß der Fall $\mu_{ija} = 0$ nicht auftreten kann, da keine der relevanten Mengen T_{rl}, T_{rl}^* leer ist.

5.4. Der Starke Existenzsatz Für SBTS

Wir verwenden wieder die Bezeichnungen von Abschnitt 5.2.

5.4.1. *Lemma.* Ist

$$h = \operatorname*{kgV}_{i \in I} (|G_i|), \tag{1}$$

so ist

$$\frac{\mu^* h}{\operatorname{ggT}(\mu^* h, \mu h, \mu\mu^*)} \mid \alpha_k(\mu, M; G). \tag{2}$$

Beweis. Existiert ein $(v, k, \mu, M; G)$-SBTS, so ist nach Proposition 2.2.2. $\mu^* \mid \mu(v-1)$, $h \mid \mu(v-1)$, also $\mu^* h \mid \operatorname{ggT}(\mu^* h, \mu h, \mu\mu^*)(v-1)$.

Daher ist für alle $v \in B_k(\mu, M; G)$

$$\frac{\mu^* h}{\operatorname{ggT}(\mu^* h, \mu h, \mu\mu^*)} \mid v - 1,$$

und nach Definition von $\alpha_k(\mu, M; G)$ folgt (2).

5.4.2. *Lemma.* Ist $\alpha_k(\mu, M; G) = 1$, so ist

$$\mu_{ij} = \mu \text{ für alle } i \neq j, \tag{3}$$

$$|G_i| \mid \mu \text{ für alle } i \in I. \tag{4}$$

Beweis. Ist $\alpha_k(\mu, M; G) = 1$, so ergibt sich aus (1) $\mu^* h = \operatorname{ggT}(\mu^* h, \mu h, \mu\mu^*)$. Insbesondere ist also $\mu^* \mid \mu$, $h \mid \mu$. Aus $\mu_{ij}|\mu^*| \mu \leqslant \mu_{ij}$ folgt dann (3), und aus $|G_i| \mid h \mid \mu$ ergibt sich (4).

Wir wollen nun umgekehrt zeigen, daß $\alpha_k(\mu, M; G) = \alpha_k(\mu; G) = 1$ ist, wenn (3) und (4) erfüllt sind.

5.4.3. *Lemma.* Angenommen, es ist

$$q = ef + 1 > e^{k(k-1)} \text{ eine Primzahlpotenz}, \tag{5a}$$

$$e \text{ gerade}, f \text{ ungerade}, \tag{5b}$$

und G erfüllt

$$|G| \mid \mu(e - r(k-2)). \tag{6}$$

Gilt dann (4), so gilt

$$rf \in B_k(\mu; G) \to q + rf \in B_k(\mu; G).$$

Beweis. Das ergibt sich sofort aus der Definition der Menge $B_k(\mu; G)$, wenn man auf die Voraussetzungen Satz 5.3.1. anwendet.

5.4.4. *Lemma.* Aus (4) folgt

$$|G| \mid \mu k, \tag{7}$$

$$\beta_k(\mu; G) \mid 2k. \tag{8}$$

Beweis. G zerlegt I in Bahnen der Länge $(G : G_i) = \frac{G}{G_i}$. Summieren wir daher über alle Bahnen G_i von I, so ist $k = \sum \frac{|G|}{|G_i|}$. Daher ist $\frac{\mu k}{|G|} = \frac{\mu}{|G|} \cdot \sum \frac{|G_i|}{G_i} = \sum \frac{\mu}{G_i}$, und aus (4) folgt, daß dies eine ganze Zahl ist. Daher gilt (7).

Weiter ergibt sich $G \mid k \cdot \mathrm{ggT}(G, \mu)$ und daher $\frac{|G|}{\mathrm{ggT}(G, \mu)} \mid k$. Wir wenden nun Satz 5.2.6. an. Es ergibt sich $\mu^* = \mu$, $e_0 = \frac{|G|}{\mathrm{ggT}(|G|, \mu)}$. Da $\beta_k(\mu; G)$ das kleinste gerade Vielfache von $e_0 \mid k$ ist, ergibt sich (8).

5.4.5. *Satz.* Ist

$$|G_i| \mid \mu \text{ für alle } i \in I,$$

so ist $\alpha_k(\mu; G) = 1$.

Beweis. Wir setzen $r = 1$, $e = 2k - 2$ und wählen eine Primzahl

$$q \equiv 2k - 1 \bmod 4k(k-1) \tag{9}$$

derart, daß

$$f = \frac{q-1}{e} \in B_k(\mu; G).$$

Nach Dirichlets Primzahlsatz ist das möglich. Denn aus (9) folgt

$$f \equiv 1 \bmod 2k, \tag{10}$$

und wegen (8) und Satz 5.2.7. ist $f \in B_k(\mu; G)$ für genügend große f mit (10), also auch für genügend große q.

Mit diesen Zahlen e, f, q, r gilt (5a, b), und (6) folgt aus (8). Daher ist nach Lemma 5.3.4. $q - rf \in B_k(\mu; G)$. Nach Definition von $\alpha_k(\mu; G)$ folgt daraus $\alpha_k(\mu; G) \mid q - rf - 1$. Aber aus den Gleichungen (2), (3) von Abschnitt 5.2. ergibt sich mit (8) $\alpha_k(\mu; G) \beta_k(\mu; G) | 2k$, so daß wegen $q - rf - 1 \equiv -1 \bmod 2k$ (das folgt aus (9), (10)) schließlich $\alpha_k(\mu; G) \mid \mathrm{ggT}(q + rf - 1, 2k) = 1$ ist. Daher ist $\alpha_k(\mu; G) = 1$.

Aus Satz 5.4.5. können wir nun in einem Spezialfall Bedingungen herleiten, die für genügend große v notwendig und hinreichend für die Existenz eines $(v, k, \mu; G)$-SBTS sind:

5.4.6. *Starker Existenzsatz für (gewisse) SBTS.* Ist

$$|G_i| \mid \mu \text{ für alle } i \in I,$$

so gibt es eine natürliche Zahl $v_k^*(\mu; G)$ derart, daß für jedes $v \geqslant v_k^*(\mu; G)$ gilt: Ein $(v, k, \mu; G)$-SBTS existiert genau dann, wenn

$$\mu v(v-1) \equiv 0 \bmod |G|. \tag{11}$$

Insbesondere gilt das für alle semiregulären Permutationsgruppen G.

Beweis. Nach Lemma 5.2.2. ist $B_k(\mu; G)$ eine kofinale Teilmenge von H_β^α. Nach Satz 5.2.6. ist β das kleinste gerade Vielfache von $\dfrac{G}{\mathrm{ggT}(|G|, \mu)}$, und nach Satz 5.4.5. ist $\alpha = 1$.

Daher ist $H_\beta^\alpha = \{v \in \mathbb{N} \mid \alpha|v-1, \beta|v(v-1)\} = \{v \in \mathbb{N} \mid \mu v(v-1) \equiv 0 \bmod |G|\}$. Nach Definition einer kofinalen Teilmenge ergibt sich daraus die Behauptung.

Wahrscheinlich gilt für jede Parameterkombination, die $(5a - c)$ aus Abschnitt 5.2. erfüllt, die Aussage (2) mit Gleichheit. Das wäre äquivalent mit der Richtigkeit der folgenden Existenzvermutung für beliebige SBTS:

Existenzvermutung für SBTS. Für jede Parameterkombination $(k, \mu, M; G)$, und für alle genügend großen natürlichen Zahlen v sind die notwendigen Bedingungen (1)–(3) von Proposition 2.2.2. für die Existenz eines $(v, k, \mu, M; G)$-SBTS auch hinreichend.

Bemerkung. Außer im behandelten Fall $|G_i| \mid \mu$ gilt die Existenzvermutung für alle Parameterkombinationen, für die aus (2) schon $\beta_k(\mu, M; G) \mid \alpha_k(\mu, M; G)$, also sogar $\alpha = \beta$, folgt. Denn dann ist $H_\beta^\alpha = \{v \in \mathbb{N} \mid v \equiv 1 \bmod \beta\}$. und Satz 5.2.7. ergibt die Behauptung. (Das gilt zum Beispiel für die Parameter der zu Roomschen Quadraten gehörigen SBTS.)

6. EINFACHE SBTS MIT $k = 3, 4$

In diesem Kapitel untersuchen wir die Existenz von einfachen SBTS mit $k = 3, 4$. (Die Existenz von primären HTS mit $k = 3$ wurde in Beispiel 2.1.5. erschöpfend behandelt.)

Im Fall $k = 3$ (Abschnitt 6.1.) können wir genaue Aussagen machen. Hier sind die notwendigen Bedingungen von Abschnitt 2.2. für einfache SBTS auch hinreichend (mit einer Ausnahme).

Für $k = 4$ dagegen (Abschnitt 6.2.) ist es nur in einigen Fällen gelungen, notwendige und hinreichende Bedingungen für die Existenz anzugeben. Jedoch wurden, wenn dies nicht gelang, im primitiven Fall unendliche Serien von SBTS angegeben. Für nichtprimäre SBTS ist der Fall der

Roomschen Quadrate gelöst, für die übrigen einfachen nichtprimitiven SBTS wurden einige wenige Beispiele angegeben. Hier bleibt noch ein weites Feld für weitere Forschungen.

6.1. Einfache SBTS Mit $k = 3$

Das folgende Diagramm enthält bis auf Isomorphie alle auf $I = \{1, 2, 3\}$ treuen Permutationsgruppen G. Wegen $|G_{ij}| = 1$ $(i \neq j)$ für alle Gruppen G sind die einfachen SBTS mit $k = 3$ gerade die $(v, 3, 1; G)$-SBTS. Außerdem enthält das Diagramm jeweils die notwendigen Bedingungen aus Proposition 2.2.2. für die Existenz eines solchen SBTS, danach die Bedingungen, unter denen eine idempotente Quasigruppe $(P, \cdot)$ durch $Q = \{(x, y, xy) \mid x, y \in P, x \neq y\}$ ein $(v, 3, 1; G)$-SBTS liefert, und schließlich äquivalente Strukturen.

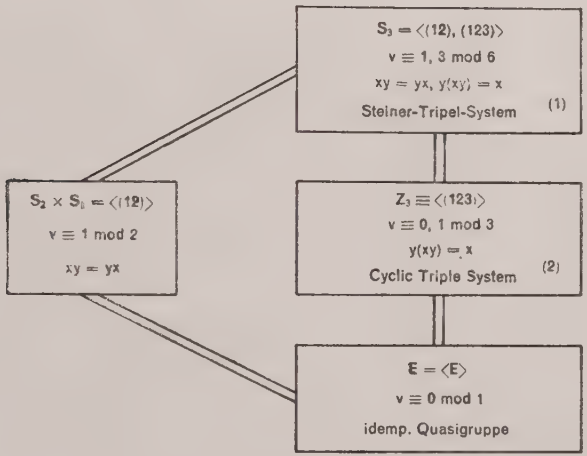

Fig. 1.

(1) Ein Steiner-Tripel-System ist ein $(v, 3, 1)$-Blockplan $(P, \mathcal{B})$. Man erhalt $\mathcal{B} = \{\{a, b, c\} \mid (a, b, c) \in Q\}$ (Satz 3.4.2.).

(2) Die Bezeichnung Cyclic Triple System für ein $(v, 3, 1; Z_3)$-SBTS stammt von Mendelsohn [14].

6.1.1. *Lemma.* Ein $(v, 3, 1; S_3)$-SBTS existiert genau dann, wenn

$$v \equiv 1, 3 \bmod 6. \tag{1}$$

Beweis. Nach 2.2.2. ist (1) notwendig. Da S_3 2-transitiv ist, erhalten wir aus jedem $(v, 3, 1)$-Blockplan ein $(v, 3, 1; S_3)$-SBTS (Satz 3.4.2.). Aber ein $(v, 3, 1)$-Blockplan existiert für $v = 1, 3 \bmod 6$ (siehe etwa Hanani [11]).

Für $v \equiv 3 \bmod 6$ können wir eine Starterkonstruktion für $(v, 3, 1; S_3)$-SBTS angeben:

6.1.2. *Lemma.* K sei abelsche Gruppe der Ordnung $2t + 1$. Dann ist

das Tupel-system, das aus den Tupeln

$$\begin{aligned}&((0, 0), (0, \epsilon), (0, -\epsilon)), \epsilon = \pm 1,\\ &\left.\begin{aligned}&((0, 0), (a, 1), (a, -1)),\\ &((-a, 1), (0, 0), (a, 1)),\\ &((a, 1), (-a, 1), (0, 0)),\end{aligned}\right\} a \in K - \{0\},\end{aligned}$$

besteht, ein $K^{\times}Z_3$-Starter für ein $(6t + 3, 3, 1)$-SBTS, und das zugehörige SBTS ist sogar ein $(6t + 3, 3, 1; S_3)$-SBTS.

Beweis. Direktes Nachrechnen.

Für den Fall $G = Z_3$ brauchen wir zwei Konstruktionen:

6 1.3. *Lemma.* K sei abelsche Gruppe der Ordnung $2t + 1$. Dann ist das aus den Tupeln

$$\begin{aligned}&\left.\begin{aligned}&((a, s + 1), (a, s), (a, s - 1)), (w, (a, s), (a, s + 1)),\\ &((a, s + 1), w, (a, s)), ((a, s), (a, s + 1), w),\end{aligned}\right\} \begin{matrix}a \in K,\\ s \bmod 3,\end{matrix}\\ &\left.\begin{aligned}&((a, s), (a + b, s + 1), (a - b, s + 1)),\\ &((a - b, s + 1), (a, s), (a + b, s + 1)),\\ &((a + b, s + 1), (a - b, s + 1), (a, s)),\end{aligned}\right\} a, b \in K, b \neq 0, s \bmod 3,\end{aligned}$$

bestehende Tupelsystem ein $(6t + 4, 3, 1; Z_3)$-SBTS über $K \times Z_3 \cup \{w\}$.

Beweis. Direkte Verifikation.

6.1.4. *Lemma.* K sei abelsche Gruppe der Ordnung $m + 4$, und $a, b, c \in K - \{0\}$ seien drei verschiedene Elemente mit $a + b + c = 0$. Dann ist mit $K' = K - \{0, a, b, c\}$ das Tupelsystem

$$Q^{\times} = \{(a, -b, 0)\} \cup \{(\infty^{(t)}, 0, t) \mid t \in K'\}$$

ein unvollständiger K-Starter für ein $((m + 4) + m, 3, 1; Z_3)$-SBTS.

Beweis. Direktes Nachrechnen.

6.1.5. *Lemma.* Ein $(v, 3, 1; Z_3)$-SBTS existiert genau dann, wenn

$$v \equiv 0, 1 \bmod 3, v \neq 6. \tag{2}$$

Beweis. Ein einfaches systematisches Probieren zeigt, daß ein $(6, 3, 1; Z_3)$-SBTS nicht existiert. Deshalb, und wegen 2.2.2. ist (2) notwendig. Wegen $B_3(1; Z_3) \supseteq B_3(1; S_3)$ folgt aus Lemma 6.1.1.:

$$v \in B_3(1; Z_3) \text{ für } v \equiv 1, 3 \bmod 6. \tag{3}$$

Aus Lemma 6.1.3. ergibt sich außerdem

$$v \in B_3(1; Z_3) \text{ für } v \equiv 4 \bmod 6. \tag{4}$$

Daher brauchen wir nur den Fall $v \equiv 0 \bmod 6$, $v > 6$ betrachten.

Es sei nun $v = 6n + 6$, $n > 0$. Wir wenden Lemma 6.1.4. mit $m = 3n + 1$, $a = 1$, $b = 2$, $c = -3$ an, wobei K die zyklische Gruppe der Ordnung

$m \neq 4$ ist. Aus Satz 4.2.6. ergibt sich dann: $v = 6n + 6$ liegt in $B_3(1; Z_3)$, falls $3n + 1 \in B_3(1; Z_3)$. Aber das letzte gilt wegen (3), (4).

6.1.6. *Lemma.* Ein $(v, 3, 1; S_2 \wr S_1)$-SBTS existiert genau dann, wenn

$$v \equiv 1 \bmod 2. \tag{5}$$

Beweis. K sei abelsche Gruppe der Ordnung $v \equiv 1 \bmod 2$. Dann ist $Q^* = \{(a, -a, 0) \mid a \in K - \{0\}\}$ ein K-Starter für ein $(v, 3, 1)$-SBTS, und das zugehörige SBTS ist sogar ein $(v, 3, 1; S_2 \wr S_1)$-SBTS.

6.1.7. *Lemma.* Ein $(v, 3, 1)$-SBTS existiert genau dann, wenn

$$v \neq 2. \tag{6}$$

Beweis. Ist $v \neq 1$, so ist $v \geqslant k = 3$. Daher ist (6) notwendig. Ist $v \neq 2$ gerade, so sei K eine abelsche Gruppe der Ordnung $v - 1$, und $t \in K - \{0\}$ fest. Dann ist das aus den Tupeln

$$(a - b, a + b, a), a, b \in K, b \neq 0, t,$$

$$(a, a + 2t, w), (a, w, a + t), (w, a + 2t, a + t), a \in K$$

bestehende Tupelsystem ein $(v, 3, 1)$-SBTS über $K \cup \{w\}$.

Wir fassen die Ergebnisse dieses Abschnitts zusammen zu:

6.1.8. *Satz.* Ein nichtleeres $(v, 3, 1; G)$-SBTS existiert genau dann, wenn

$$v \geqslant 3, v - 1 \equiv 0 \bmod |G|, v(v-1) \equiv 0 \bmod |G|, \tag{7}$$

mit der Ausnahme des nichtexistierenden $(6, 3, 1; Z_3)$-SBTS.

Beispiel 2.1.5. enthält $(v, 3, 1; S_3)$-HTS für alle natürlichen Zahlen v; daraus ergibt sich sofort.

6.1.9. *Satz.* Ein $(v, 3, 1; G)$-HTS existiert für alle treuen Permutationsgruppen G vom Grad 3 und alle natürlichen Zahlen v.

6.2 Einfache SBTS mit $k = 4$

Das folgende Diagramm enthält bis auf Isomorphie alle auf $I = \{1, 2, 3, 4\}$ treuen Permutationsgruppen G, dann die Parameter des zugehörigen einfachen SBTS, die notwendigen Bedingungen aus Proposition 2.2.2. für dessen Existenz. Im Fall primitiver SBTS folgen dann die Bedingungen für zwei Quasigruppen $(P, \cdot)$, $(P, \circ)$, die durch

$$Q = \{(x, xy, y, x \circ y) \mid x, y \in P, x \neq y\}$$

ein solches SBTS liefern. Danach folgen wieder andere kombinatorisch äquivalente Strukturen.

Ist M nicht angegeben, so ist $M = (\mu)$; die anderen Matrizen M sind

$$M_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}.$$

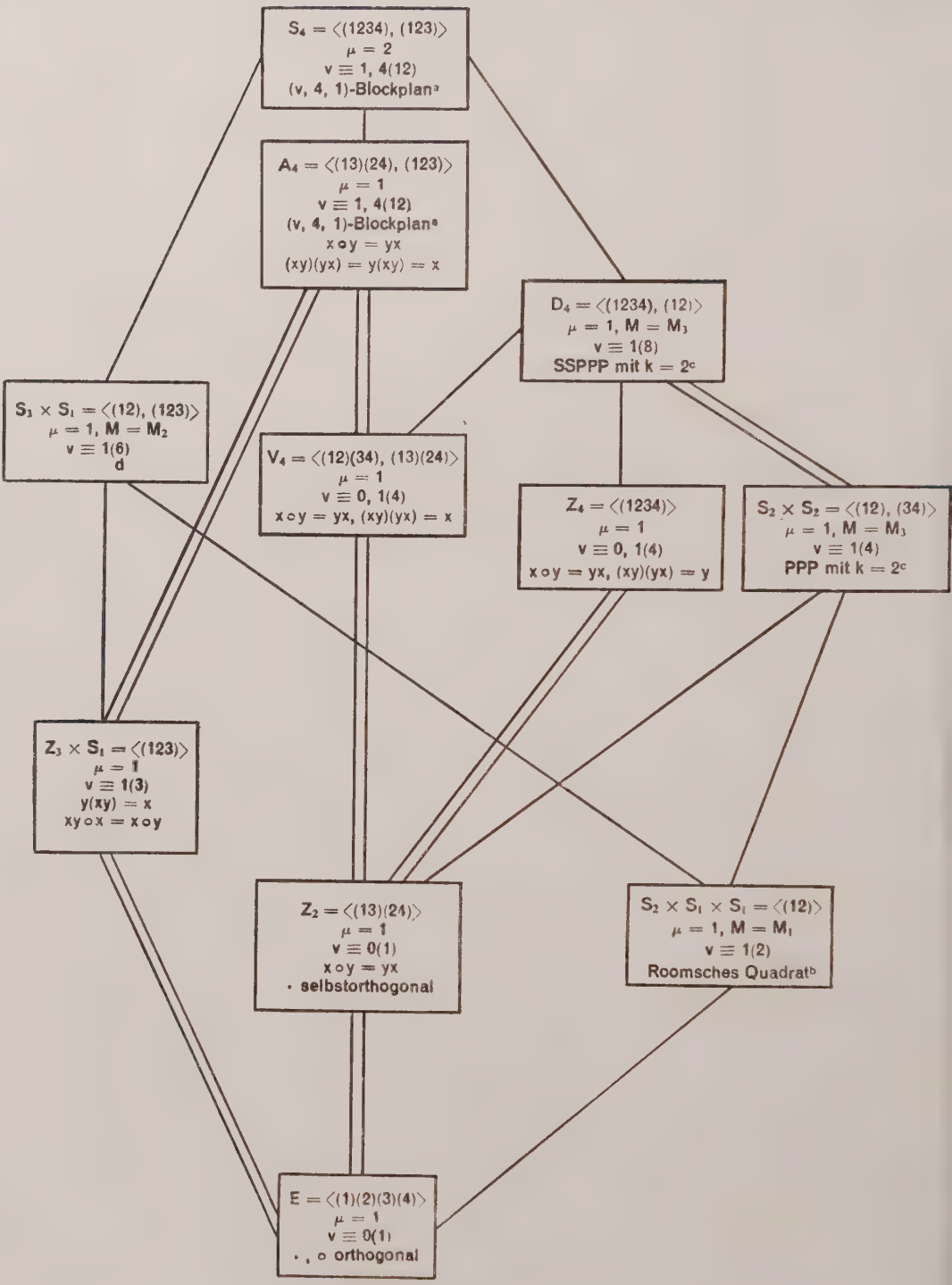

Fig. 2

(a) $(P, \mathcal{B})$ mit $\{a, b, c, d\} \in \mathcal{B} \Leftrightarrow (a, b, c, d) \in Q$, nach Satz 3.4.2.
(b) $\{a, \infty\}$ in Zelle (a, a); $\{a, b\}$ in Zelle $(i, j) \Leftrightarrow (a, b, i, j) \in Q$, nach Satz 3.5.4.
(c) (SS) PPP = (self symmetric) paired partial plane, s. Anhang.
(d) Dazu gehört ein halbauflösbares Steiner-Tripel-System, s. Anhang.

Wir betrachten zuerst den primären Fall.

Fall $G = A_4$. Da A_4 2-transitiv ist, ist nach Satz 4.3.2. ein $(v, 4, 1; A_4)$-SBTS zu einem $(v, 4, 1)$-Blockplan äquivalent. Ein solcher existiert aber genau dann, wenn $v \equiv 1, 4 \bmod 12$ (siehe etwa Hanani [11]). Also gilt:

6.2.1. *Lemma.* Ein $(v, 4, 1; A_4)$-SBTS existiert genau dann, wenn

$$v \equiv 1, 4 \bmod 12. \tag{1}$$

Fall $G = V_4$. Wegen $B_4(1; V_4) \supseteq B_4(1; A_4)$ ist

$$v \in B_4(1; V_4) \text{ für } v \equiv 1, 4 \bmod 12. \tag{2}$$

Ist $K = GF(2^i)$, $i > 1$, $t \in K - \{0, 1\}$, so ist

$$Q = \{(a, ta + (1-t)b, b, (1-t)a + tb) \mid a, b \in K, a \neq b\}$$

ein $(2^i, 4, 1; V_4)$-SBTS über K, und daher

$$2^i \in B_4(1; V_4) \text{ für alle } i > 1. \tag{3}$$

Eine direkte Rechnung zeigt

$$5 \notin B_4(1; V_4). \tag{4}$$

Da aus Proposition 2.2.2.

$$B_4(1; V_4) \subseteq \{v \in \mathbb{N} \mid v \equiv 0, 1 \bmod 4\} \tag{5}$$

folgt, sind die ersten unentschiedenen Fälle

$$v = 9, 12, 17, 20, 21, 24.$$

Fall $G = Z_4$. Ist K eine abelsche Gruppe der Ordnung $v \equiv 1 \bmod 4$, und σ ein Automorphismus mit $\sigma^2 = -1$, so ist

$$Q = \{(a + b, a + \sigma b, a - b, a - \sigma b) \mid a, b \in K, b \neq 0\}$$

ein $(v, 4, 1; Z_4)$-SBTS. Ein solcher Automorphismus existiert, wenn K das direkte Produkt der additiven Gruppen von endlichen Körpern $GF(q)$, $q \equiv 1 \bmod 4$, ist, denn für die letzteren kann man für σ eine primitive vierte Einheitswurzel nehmen. Daher ist

$$v \in B_4(1; Z_4), \text{ wenn } v \text{ Produkt von Primzahlpotenzen } q \equiv 1 \bmod 4 \text{ ist.} \tag{6}$$

Eine direkte Rechnung ergibt

$$4 \notin B_4(1; Z_4). \tag{7}$$

Da aus Proposition 2.2.2.

$$B_4(1; Z_4) \subseteq \{v \in \mathbb{N} \mid v \equiv 0, 1 \bmod 4\} \tag{8}$$

folgt, sind die ersten unentschiedenen Fälle

$$v = 8, 12, 16, 20, 21, 24.$$

Fall $G = Z_3 \times S_1$. Wegen $B_4(1; Z_3 \times S_1) \supseteq B_4(1; A_4)$ ist

$$v \in B_4(1; Z_3 \times S_1), \text{ wenn } v \equiv 1, 4 \bmod 12. \tag{9}$$

Ist K eine abelsche Gruppe der Ordnung $v \equiv 1 \bmod 3$, die einen Automor-

phismus ρ mit $\rho^2 + \rho + 1 = 0$ besitzt, so ist

$$Q = \{(3a, 3b, 3c, a + b + c) \mid a + \rho b + \rho^2 c = 0, \text{ nicht } a = b = c\}$$

ein $(v, 4, 1; Z_3 \times S_1)$-SBTS. In einem endlichen Körper $GF(q)$, $q \equiv 1 \bmod 3$, kann man für ρ eine primitive dritte Einheiswurzel nehmen; daher existiert ein Automorphismus der geforderten Art im direkten Produkt solcher Körper, und es ist

$$v \in B_4(1; Z_3 \times S_1), \text{ wenn } v \text{ Produkt von Primzahlpotenzen } q \equiv 1 \bmod 3 \text{ ist.} \quad (10)$$

Da aus Proposition 2.2.2.

$$B_4(1; Z_3 \times S_1) \subseteq \{v \in \mathbb{N} \mid v \equiv 1 \bmod 3\} \quad (11)$$

folgt, sind die ersten unentschiedenen Fälle

$$v = 10, 22, 34, 40, 46, 55.$$

Fall $G = Z_2$. Wir zeigen.

6.2.2. *Lemma.* Ein $(v, 4, 1; Z_2)$-SBTS existiert genau dann, wenn

$$v \neq 2, 3, 6. \quad (12)$$

Beweis. Brayton, Coppersmith und Hoffmann haben gezeigt [3], daß selbstorthogonale lateinische Quadrate der Ordnung v genau dann existieren, wenn $v \neq 2, 3, 6$. Nach 3.3.7. (c) existiert also ein $(v, 4, 1; Z_2)$-HTS genau für $v \neq 2, 3, 6$. Es genügt daher zu zeigen. daß aus der Existenz eines $(v, 4, 1; Z_2)$-HTS Q die Existenz eines $(v, 4, 1; Z_2)$-SBTS gefolgert werden kann (die Umkehrung ist klar).

Es gibt nun für alle $a \in P$ genau ein Tupel $(a, \pi a, a, \pi' a) \in Q$. Wegen $(13)(24) \in Z_2$ folgt $\pi' a = a$. Ist nun $(b, \pi a, c, \pi a) \in Q$, so muß wegen $\mu = 1$, $b = c = a$ sein. Daher ist π eine Permutation. Wegen $(a, a, a, a) \in \pi^{-1}Q$ für alle $a \in P$ ist $\pi^{-1}Q$ idempotent. $\pi^{-1}Q$ hat aber immer noch den freien Automorphismus $(13)(24)$, und das zugehörige SBTS ist daher ein $(v, 4, 1; Z_2)$-SBTS. Damit ist das Lemma bewiesen.

Fall $G = E$. Hier gilt.

6.2.3. *Lemma.* Ein $(v, 4, 1)$-SBTS existiert genau dann, wenn

$$v \neq 2, 3, 6. \quad (13)$$

Beweis. Aus 6.2.2. folgt, daß (13) hinreichend ist. Andrerseits ist für $v \neq 1$ schon $v \geqslant k = 4$, also $v \neq 2, 3$. Schließlich kann ein $(6, 4, 1)$-SBTS nicht existieren, da ein solches auf ein Paar (idempotenter) Lateinischer Quadrate der Ordnung 6 führen würde. Das ist aber unmöglich (Tarry [24]).

Fall $G = S_4$. Da S_4 2-transitiv ist, schließt man ebenso wie bei A_4:

6.2.4. *Lemma.* Ein $(v, 4, 2; S_4)$-SBTS existiert genau dann, wenn

$$v \equiv 1, 4 \bmod 12. \quad (14)$$

Fall $G = S_2 \times S_1 \times S_1$. Beispiel 4.2.4. ergibt

$q \in B_4(1, M_1; S_2 \times S_1 \times S_1)$ für alle ungeraden Primzahlpotenzen q. (15)

Da ein $(v, 4, 1, M_1; S_2 \times S_1 \times S_1)$-SBTS zu einem Roomschen Quadrat der Seite v äquivalent ist (Satz 3.5.4.), und dieses für alle ungeraden $v \neq 3, 5$ existiert (siehe etwa Wallis [26]), folgt.

6.2.5. *Lemma.* Ein einfaches $(v, 4, 1, M_1; S_2 \times S_1 \times S_1)$-SBTS existiert genau dann, wenn

$$v \equiv 1 \bmod 2, v \neq 3, 5. \tag{16}$$

Schließlich kenne ich für die Gruppen D_4, $S_2 \times S_2$ und $S_3 \times S_1$ keine einfache Serie, die unendlich viele SBTS mit diesen Gruppen liefert. Aber der schwache Existenzsatz für SBTS (5.2.7.) garantiert hier wenigstens, daß die im Diagramm angegebenen notwendigen Bedingungen für genügend große v auch hinreichend sind.

Wir geben jedoch auch für einige kleine Werte von v Starter für solche SBTS:

6.2.6. *Beispiele.* (a) $\{(0, 1, 3, 2)\}$ ist ein Z_7-Starter für ein einfaches $(7, 4, 1, M_2; S_3 \times S_1)$-SBTS.

(b) $\{(0, 1, 4, 2), (2, 7, 9, 0)\}$ ist ein Z_{13}-Starter für ein einfaches $(13, 4, 1, M_2; S_3 \times S_1)$-SBTS.

(c) $\{(0, 1, 2, 4)\}$ ist ein Z_5-Starter für ein einfaches $(5, 4, 1, M_3; S_2 \times S_2)$-SBTS.

(d) $\{(0, 1, 2, 4)\}$ ist ein Z_9-Starter für ein einfaches $(9, 4, 1, M_3; D_4)$-SBTS.

ANHANG

BEMERKUNGEN, WEITERE ERGEBNISSE, UND OFFENE PROBLEME

(zu Kapitel 2) Der Begriff des Tupelsystems kann in mehreren Richtungen verallgemeinert werden. Zum einen kann man "Tupelsysteme mit Lücken" betrachten, in denen die Abbildung ϵ nicht auf ganz $Q \times I$ definiert ist. Dann kann man die Abbildung ϵ durch eine dreistellige Relation σ in $Q \times I \times P$ ersetzen, und das zu $X \in Q$ gehörige Tupel enthält dann als Eintrag an der Stelle i anstelle eines Punktes eine Punktmenge

$$X_i = \{a \in P \mid \sigma(x, i, a)\}.$$

Schließlich kann man Tupelsysteme betrachten, in denen statt einer Punktmenge P ein k-Tupel $(P_i : i \in I)$ gegeben ist, und die Einträge der Tupel an Stelle i in P_i liegen. Diese Erweiterung läßt dann Mengen P_i mit verschiedenen Mächtigkeiten zu und spielt für Homotopiebetrachtungen eine Rolle.

Nichtidempotente homogene Tupelsysteme wurden nicht systematisch untersucht. Die Ungleichung 2.2.10. ist (für orthogonale Arrays) bekannt,

s. etwa Raghavarao [21]. Als eine hinreichende Bedingung für die Existenz von HTS vermute ich:

Problem 1: Existiert für alle $v \geqslant 1, 3 \leqslant k \leqslant 4\mu - 1$ ein (v, k, μ)-HTS? ■

zu bejahen ist. Für $k = 3$ folgt das aus Beispiel 2.1.5., für $k \leqslant 7$ wurde es von Hanani [11] gezeigt. Offensichtlich genügt es, für alle v, μ ein $(v, 4\mu - 1, \mu)$-HTS anzugeben. Eine allgemeine Lösung des Problems würde die Existenz von Hadamardmatrizen der Ordnung 4μ implizieren ($v = 2$, s. unten).

Die möglichen freien Automorphismengruppen von nicht-idempotenten HTS werden im Fall $\mu = 1$ von Neumaier [18] klassifiziert; im allgemeinen Fall ist nichts dazu bekannt.

Problem 2: Klassifiziere die möglichen freien Automorphismen-gruppen für (v, k, μ)-HTS, $\mu > 1$. ■

Auf Transversalen in HTS und SBTS wurde nicht weiter eingegangen. Auch auflösbare Tupelsysteme (das sind Tupelsysteme, die in disjunkte Transversalen zerlegt werden können, die eine Verträglichkeitsbedingung mit der freien Automorphismengruppe erfüllen) wurden nicht behandelt.

(zu Kapitel 3) Analog wie für Transversalpläne kann man auch beliebige GDD als Tupelsysteme darstellen, allerdings als solche mit "Lücken" (s.o.).

Einbettungssätze für Netze in affine Ebenen beweist Bruck [4]. In die Sprache der HTS übersetzt lauten seine Ergebnisse: (a) Ein $(v, v + 1 - d, 1)$-HTS mit $v > \frac{1}{2}(d - 1)(d^3 - d^2 + d + 2)$ kann eindeutig durch Hinzufügen von Stellen zu einem $(v, v + 1, 1)$-HTS ergänzt werden. (b) Ein $(v, v + 1 - d, 1)$-HTS mit $v > (d - 1)^2$ kann auf höchstens eine Weise zu einem $(v, v + 1, 1)$-HTS ergänzt werden.

Man kann auf dieselbe Weise wie für Blockpläne auch den t-Blockplänen Tupelsysteme zuordnen, bei denen dann auch höhere Situationszahlen (bis zur Stufe t) konstant sind. Jedoch ist die Theorie für solche t-SBTS wesentlich komplizierter und kann hier nicht auseinandergesetzt werden. Dasselbe gilt natürlich auch für orthogonale Arrays, die auf "t-HTS" führen.

Problem 3. Entwickle eine Theorie der t-(v, k, μ)-HTS und-SBTS. ■

Satz 3.4. (b) steht in engem Zusammenhang mit einer Arbeit von Ganter und Werner [7] über die Koordinatisierung von Blockplänen mit Methoden der universellen Algebra. Die zu den $(v, q, 1; A(q))$-SBTS nach Satz 3.3.6. gehörigen Quasigruppen sind in ihrem Sinn koordinatisierend.

Problem 4. Charakterisiere die minimal darstellbaren Blockpläne. ■

Problem 5. Existiert für alle natürlichen Zahlen n ein $(4n - 1, 2n - 1,$

$n-1$; D_n)-SBTS? (Daraus würde die Existenz eines Hadamard-Blockplans und damit einer Hadamardmatrix der Ordnung $4n$ folgen.) ■

Die Äquivalenz von Roomschen Quadraten mit bestimmten einfachen SBTS läßt sich ohne weiteres auf Roomsche t-designs (s. Wallis [25]) erweitern. Auch für andere Klassen einfacher SBTS kann man äquivalente Strukturen erhalten. So kann man für $G = S_{k_1} \times \ldots \times S_{k_n}$ die auf die G-Bahnen von I beschränkten SBTS als Inzidenzstrukturen auffassen (analog wie primitive SBTS auf Blockpläne) und deren Eigenschaften beschreiben. Für die einfachen SBTS mit $G = S_k \times S_1$ und $G = S_k \times S_k$ ergeben sich auf diese Weise sog. "teilweise auflösbaren Blockpläne" bzw. "paired partial planes".

Ordnet man die 4μ Tupel eines $(2, 4\mu - 1, \mu)$-HTS untereinander an, ersetzt jede 0 durch -1, und ergänzt die entstehende Matrix durch eine Spalte mit lauter Einsen, so ergibt sich eine Hadamard-Matrix. Da umgekehrt jede Hadamardmatrix durch Multiplikation der Zeilen mit ± 1 so transformiert werden kann, daß in der letzten Spalte lauter Einsen stehen, ist diese Konstruktion umkehrbar.

Die Darstellung von semiregulären GDD durch unvollständige HTS (s. unten) kann hier nicht besprochen werden, und wird in einer spätern Arbeit behandelt.

Schließlich bemerken wir, daß ein $(v, k, 1)$-HTS auch aufgefaßt werden kann als ein equidistanter Blockcode mit v^2 Codeworten über einer v-Menge P, der Hammingdistanz $d = k - 1$ hat. (Für die Begriffe s. etwa Berlekamp [1] oder Peterson/Weldon [19]).

(zu Kapitel 4) Eine Schwierigkeit bei der direkten Konstruktion von Tupelsystemen mit algebraischen Methoden ist, daß bei Verwendung von Körpern der Parameter v auf eine Primzahlpotenz festgelegt ist. Um dies zu vermeiden, kann man nun auf die Assoziativität verzichten, und sich mit schwächeren Forderungen begnügen. Wir führen dies in einer späteren Arbeit aus und beweisen zu den Sätzen in Abschnitt 4.1. analoge Sätze, die Fastvektorräume anstelle von Körpern benutzen. (Die Fastvektorräume sind so definiert, daß sie außer den Vektorräumen noch genügend Beispiele, insbesondere auch von Nichtprimzahlordnung enthalten.)

Starterverfahren sind—meist unter dem Namen "method of differences"—ein bekanntes Mittel zur Konstruktion von kombinatorischen Designs. Für orthogonale Arrays s. etwa Wilson [32], Raghavarao [21], für lateinische Quadrate Jungnickel [12], für Blockpläne Hanani [11], Wilson [28], für Roomsche Quadrate Wallis [25], Neumaier [17]. (Die Liste enthält nur eine kleine Auswahl aus den vielen möglichen Referenzen.) Beispiel 4.2.4. ist eine Übertragung einer Konstruktion von Mullin und Nemeth (s. Wallis [25]), und 4.2.7. stammt von Parker (s. Raghavarao [21]).

Eine interessante Frage ist, unter welchen Bedingungen aus der Existenz von Startern für eine abelsche Gruppe H und für K/H die Existenz eines

Starters für K folgt (Produkt-konstruktion). In dieser Hinsicht liegen für klassische Fälle einige Resultate vor (Gross/Leonard [8], Jungnickel [12], Neumaier [17]).

Problem 6. Gib Produktkonstruktionen für weitere Klassen von Startern an. ■

Problem 7. Bestimme die Gruppen K, für die ein K-Starter für ein $(v, k, \mu; G)$-SBTS existiert. Sind das, bis auf endlich viele Ausnahmen, alle, die die notwendigen Bedingungen für $v = |K|$ erfüllen ? ■

Von den vielen rekursiven Konstruktionen wurden hier nur einige bracht (so fehlt z.B. die Moore-Konstruktion, Moore [16]). Für einige systematische Theorie braucht man neue Begriffe: Abgeschlossene Punktmengen, Untertupelsysteme und unvollständige HTS. Die rekursiven Konstruktionen lassen sich dann durch einen Vervollständigungsprozeß von unvollständigen HTS beschreiben. Die Einzelheiten sollen in einer anderen Arbeit beschrieben werden.

Alle mir bekannten rekursiven Konstruktionen lassen entweder k fest oder vergrößern k und μ gleichzeitig.

Problem 8. Finde rekursive Konstruktionen für HTS (SBTS), die v, k vergrößern und μ festlassen. ■

Für Blockpläne, Hadamardmatrizen und Roomsche Quadrate gibt es jeweils eine ganze Reihe von Konstruktionen. Einige davon lassen sich (manchmal nicht ganz offensichtlich) auf größere Klassen von Tupelsystemen übertragen. So ist z.B. die Konstruktion 4.3.3. eine Übertragung der Verdopplungs-konstruktion für Hadamardmatrizen. (Die Kroneckerprodukt-konstruktion kann auf ähnliche Weise übertragen werden.)

Problem 9. Übertrage bekannte Konstruktionen von Blockplänen, Hadamardmatrizen oder Roomschen Quadraten auf HTS order SBTS ! ■

(zu Kapitel 5).

Problem 10. Beweise die allgemeine Existenzvermutung für SBTS. ■

Für $(v, k, \mu; G)$-SBTS ergibt sich, ähnlich wie in Lemma 5.4.4. $\beta \mid k(k-1)$ und $\alpha^* = (\beta, k-1)$, wobei α^* der vermutete Wert von α aus Lemma 5.4 1. ist. Damit kann man leicht zeigen, daß $\alpha = \alpha^*$ ist, falls nur *ein* durch k teilbares $v \in B_k(\mu; G)$ existiert. (Das löst das Problem z.B. für $G = S_k$, wo das Tupelsystem aus allen Permutationen von k Elementen ein $(k, k, 1; S_k)$-SBTS ist!).

Problem 11. Konstruiere $(v, k, \mu; G)$-SBTS mit $k \mid v$. ■

(zu Kapitel 6) Konstruktion 6.1.2. ist eine Übertragung einer Konstruktion von Skolem [23]. Der Fall $G = V_4$ wurde von Moore [16] für $v \equiv 0 \mod 4$ under dem Namen "triple-whist tournament arrangements" untersucht. Der Fall $G = Z_3$ wird in Mendelsohn [14] unter dem Namen "cyclic triple system" eingeführt.

Problem 12. Bestimme (durch rekursive und direkte Verfahren) notwendige und hinreichende Bedingungen für die Existenz von $(v, 4, 1; G)$-SBTS, $G = V_4, Z_4, Z_3 \times S_1$. ■

Problem 13. Gib unendliche Serien für einfache $(v, 4, 1, M; G)$-SBTS, $G = S_3 \times S_1, S_2 \times S_2, D_4$ an. (Aus der PBD-Konstruktion und den angegebenen Beispielen ergeben sich solche Familien; gefragt ist also nach direkten Konstruktionen.) ■

Problem 14. Konstruiere nichtidempotente $(v, k, 1; G)$-HTS für $G = Z_3 \times S_1, V_4, Z_4$. (Für $G = E, Z_2$ ist das Spektrum der möglichen v schon durch idempotente HTS erfüllt; für $G = A_4$ sind alle primitiven HTS idempotent.) ■

Bemerkung

Diese Arbeit wurde als Inaugural-Dissertation zur Erlangung der Doktorwärde der Mathematisch-Naturwissenschaftlichen Fakultät der Freien Universität Berlin akzeptiert.

References

[1] E. R. Berlekamp (1968), *Algebraic Coding Theory*, McGraw-Hill, New York.

[2] R. C. Bose, S. S. Shrikhande and E. T. Parker (1960), "Further results on the construction of mutually orthogonal Latin squares and the falsity of a conjecture of Euler", *Can. J. Math.*, **12**, 189–203.

[3] R. K. Brayton, D. Coppersmith and A. J. Hoffman (1974), "Self-orthogonal Latin squares of all orders $n \neq 2, 3, 6$", *Bull. Amer. Math. Soc.*, **80**, 116–118.

[4] R. H. Bruck (1963), "Finite nets, II: Uniqueness and embedding", *Pac. J. Math.*, **13**, 421–457.

[5] P. Dembowski (1968), *Finite Geometries*, Springer, Berlin-Heidelberg-New York.

[6] J. Dénes and A. D. Keedwell (1974), *Latin Squares and Their Applications*, Akadémiai Kiadó, Budapest.

[7] B. Ganter and H. Werner (März, 1973), "Equational classes of Steiner systems", Preprint Nr. 56, TH Darmstadt,

[8] K. B. Gross and P. A. Leonard, "Adders for the patterned starter in nonabelian groups", *J. Austr. Math. Soc.* (erscheint dort).

[9] M. Hall Jr. (1967), *Combinatorial Theory*, Blaisdell, Waltham, Mass.

[10] H. Hanani (1961), "The existence and construction of balanced incomplete block designs", *Ann. Math. Statist.*, **32**, 361–386.

[11] H. Hanani (1975), "Balanced incomplete block designs and related designs", *Discr. Math.*, **11**, 255–369.

[12] D. Jungnickel, "On difference matrices and regular Latin squares" (Dezember 1975), *Kombinatorik*, Preprint Nr. 3, Berlin.

[13] J. F. Lawless (1971), "Pairwise balanced designs and the construction of certain combinatorial systems", in: Proc. 2nd Louisiana Conf. Graph theory, Combinatorics, Computing.

[14] N. S. Mendelsohn (1970), "Orthogonal Steiner systems", *aequat. math.*, **5**, 268–272.

[15] E. H. Moore (1893), "Concerning triple systems", *Math. Ann.*, **43**, 271–285.

[16] E. H. Moore (1896), "Tactical memoranda I–III", *Amer. J. Math.*, **18**, 264–303.

[17] A. Neumaier, "On transitive commutative idempotent quasigroups", erscheint in: *J. Austr. Math. Soc.*

[18] A. Neumaier, "Affine Ebenen und Tupelsysteme", erscheint in: *Geometriae dedicata.*

[19] W. W. Peterson and E. S. Weldon Jr. (1972), *Error Correcting Codes*, 2nd ed., MIT Press, Cambridge, Mass.

[20] K. Prachar (1957), *Primzahlverteilung*, Springer, Berlin-Göttingen-Heidelberg.

[21] D. Raghavarao (1971), *Constructions and Combinatorial Problems in Design of Experiments*, Wiley, New York.

[22] H. J. Ryser (1963), *Combinatorial Mathematics*, Wiley, New York.

[23] Th. Skolem (1958), *Math. Scand.*, **6**, 273–280.

[24] G. Tarry (1900), "Le problème des 36 officiers", *Compt. Rend. Assoc. Av. Sci.*, (1901), **1**, 122–123; **2**, 170–203.

[25] W. D. Wallis (1972), "Room squares", in: Wallis, W. D. *et al.*, "Combinatorics: Room squares, sum-free sets, Hadamard matrices", Lecture Notes in Mathematics 292, Springer, Berlin-Heidelberg-New York.

[26] W. D. Wallis and R. C. Mullin (Oct. 1974), "The Existence of Room Squares", Research Report No. 129, Newcastle.

[27] R. M. Wilson (1972), "Cyclotomy and difference families in elementary abelian groups", *J. Number Theory*, **4**, 17–47.

[28] R. M. Wilson (1972), "An existence theory for pairwise balanced designs, I: Composition theorems and morphisms", *J. Comb. Th.*, **A13**, 220–245.

[29] R. M. Wilson (1972), "An existence theory for pairwise balanced designs, II: The structure of PBD-closed sets and the existence conjectures", *J. comb. Th.*, **A13**, 246–273.

[30] R. M. Wilson (1975), "An existence theory for pairwise balanced designs, III: Proof of the existence conjectures", *J. comb. Th.*, **A18**, 71–79.

[31] R. M. Wilson (1974), "Construction and uses of pairwise balanced designs", in: Combinatorics, Part 1, Math. Centre Tracts 55, Amsterdam, pp. 18–41.

[32] R. M. Wilson (1975), "A few more squares", in: Proc. 5th SE Conf. Combinatorics, Graph Theory, Computing.

[Received : November, 1976]